Can *Brandenburg v. Ohio* Survive the Internet and the Age of Terrorism?: The Secret Weakening of a Venerable Doctrine

CHRIS MONTGOMERY*

I. INTRODUCTION

At this distance from the terrorist attacks of September 11, 2001, it is not a stretch to say that whatever imminent, unknowable peril the country was in at that moment has largely subsided. While the terrorist threat to the United States still exists, the full power of the federal government is now employed against that threat through such mechanisms as the Authorization for Use of Military Force,[1] Patriot Act,[2] and Foreign Intelligence Surveillance Act.[3]

Terrorists have not attacked the country since 9/11, although government officials have publicized numerous nascent plots by Islamic radicals during the past several years that seem to indicate that they are still trying. The general picture that has emerged from those foiled plots, however, is hardly one that inspires existential dread. Rather, these "terrorists" could better be described, in most instances, as disorganized bands of small time criminals and sundry other disaffected individuals who may be long on intent, but are very short on operational capabilities.[4]

This is not to say that the terrorist threat in this country is nonexistent, only that it is largely contained.[5] And it is widely recognized that the Muslim-American population poses less of a threat and is better assimilated into U.S. culture than Muslim populations in other countries, particularly in

---

* Articles Editor, Ohio State Law Journal; J.D. Candidate, 2009, The Ohio State University Moritz College of Law; B.A., History, magna cum laude, 1999, Princeton University; M.A., Journalism, Northwestern University Medill School of Journalism, 2000.

[1] Pub. L. No. 107-40, 115 Stat. 224 (2001).

[2] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified in scattered sections of the U.S.C.).

[3] Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended in scattered sections of 18 U.S.C.).

[4] *See infra* Part IV.

[5] Steve Chapman, Editorial, *Terrorism Crisis Has Passed; Potential Targets Need Vigilance, Not Ongoing Panic*, CHI. TRIB., July 12, 2007, at 21. Chapman maintains that the terrorist threat is "not a danger on the order of Nazi Germany or the Soviet Union or even Saddam Hussein. It's more like organized crime—an ongoing problem demanding unceasing vigilance, a malady that can be contained but never eliminated." *Id.*

Europe.[6] The scale of the threat to the United States matters. Dangerous times have tended time and again during the nation's history to lead to bad law, particularly when it comes to civil liberties. This Note considers specifically the freedom of speech and the constitutional standard for speech that advocates criminal acts. The modern standard was established by the Supreme Court in *Brandenburg v. Ohio*,[7] and commentators have roundly described it, at least in theory, as extraordinarily protective of free speech.[8] But in order to arrive at that standard, the Court had to redefine fifty years of jurisprudence crafted in response to various threats—perceived and real—inside and outside the country.[9]

The Court decided the cases leading up to *Brandenburg* against a backdrop of demographic and technological change in the country that heightened government fears about the breakdown of social cohesion and the rise of corruption and violence.[10] In the years before and during World War I, those fears were generated by waves of European immigrants and the rise of new technologies such as the telephone, telegraph, and direct mail.[11] During the Cold War, it was the children of those immigrants and the increasing pervasiveness of new technologies such as radio that stoked fears of foreign interference in U.S. affairs.[12]

The country is prone to the same types of fears today, growing out of the same root causes: immigration, especially of Muslim Americans; and

---

[6] MITCHELL D. SILBER & ARVIN BHATT, N.Y. CITY POLICE DEP'T, RADICALIZATION IN THE WEST: THE HOMEGROWN THREAT 56 (2007) (noting that "[t]he United States has appeared to be somewhat immune" from the process of radicalization of its Muslim population); PEW RESEARCH CTR., MUSLIM AMERICANS: MIDDLE CLASS AND MOSTLY MAINSTREAM 19 (2007) (noting that a "nationwide survey of Muslim Americans finds them to be largely assimilated, happy with their lives, and moderate with respect to many of the issues that have divided Muslims and Westerners around the world"); *see also* Peter Skerry, *The American Exception: Why Muslims in the U.S. Aren't As Attracted to Jihad as Those in Europe*, TIME, Aug. 21, 2006, at 30.

[7] 395 U.S. 444, 447 (1969) (holding that government shall not "forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action").

[8] *E.g.*, Mark Tushnet, *Defending* Korematsu*?: Reflections on Civil Liberties in Wartime*, 2003 WIS. L. REV. 273, 286–87 (2003); David Crump, *Camouflaged Incitement: Freedom of Speech, Communicative Torts, and the Borderland of the* Brandenburg *Test*, 29 GA. L. REV. 1, 12–13 (1994).

[9] Geoffrey R. Stone, *War Fever*, 69 MO. L. REV. 1131, 1152 (2004).

[10] Peter Margulies, *The Clear and Present Internet: Terrorism, Cyberspace, and the First Amendment*, 2004 UCLA J.L. & TECH. 4, 5–6 (2004).

[11] *Id.* at 12–16.

[12] *Id.* at 22.

technology, particularly the Internet Government officials worry that the Internet aids the radicalization process of disaffected individuals, increasing the likelihood that they will eventually turn to terrorist tactics.[13] And just as the United States is under similar pressures today as in the past, there is the same possibility of resorting to heavy-handed laws and tactics to deal with the perceived threat. As Professor Stone put it, "[a]gain and again, Americans have allowed fear to get the better of them" by curtailing civil liberties in times of danger.[14] The country's learning curve seemingly always trails just behind current events, as cogently noted by Professor Tushnet.[15] In response to curtailment of civil liberties, "[j]udges and scholars develop doctrines and approaches that preclude the repetition of the last generation's mistakes."[16] Then, new threats emerge that cause new policy responses not precluded by the old doctrines, and the "next generation again concludes that the new policy responses were mistaken."[17] Tushnet concluded that "[w]e learn from our mistakes to the extent that we do not repeat precisely the same errors, but it seems that we do not learn enough to keep us from making new and different mistakes."[18]

The federal government might already have gone too far in several aspects of its "war on terror," including warrantless wiretapping,[19] using the Patriot Act to improperly obtain personal information about people in the United States,[20] and aggressive prosecutions under a provision that bans

---

[13] *See* SILBER & BHATT, *supra* note 6, at 8; *see also* Press Release, Office of the Dir. of Nat'l Intelligence, Declassified Key Judgments of the National Intelligence Estimate "Trends in Global Terrorism: Implications for the United States" (Apr. 2006), *available at* http://www.dni.gov/press_releases/Declassified_NIE_Key_Judgments.pdf.

[14] Stone, *supra* note 9, at 1131.

[15] Tushnet, *supra* note 8, at 292.

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] *See* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1; Barton Gellman, Dafna Linzer & Carol D. Leonnig, *Surveillance Net Yields Few Suspects; NSA's Hunt for Terrorists Scrutinizes Thousands of Americans, but Most Are Later Cleared*, WASH. POST, Feb. 5, 2006, at A1; PETER SWIRE, CTR. FOR AM. PROGRESS, LEGAL FAQS ON NSA WIRETAPS (2006), http://www.americanprogress.org/issues/2006/01/b1389573.html ("Based on facts available to date, the wiretap program appears to be clearly illegal.").

[20] *See infra* Part V.B.3; *see also* David Johnston & Eric Lipton, *U.S. Report To Fault Wide Use of Special Subpoenas by F.B.I.*, N.Y. TIMES, Mar. 9, 2007, at A1; John Solomon & Barton Gellman, *Frequent Errors in FBI's Secret Records Requests; Audit Finds Possible Rule Violations*, WASH. POST, Mar. 9, 2007, at A1.

providing "material support" to terrorists.[21] But however valid the argument that such government activities have "chilled" or discouraged speech of individuals critical of U.S. policies, it is axiomatic that the government is not attempting to suppress the types of speech that it has during previous times of war. The *Brandenburg* doctrine effectively limits prosecutions for speech and speech activities that are not directed to, or likely to result in, imminent law violation.[22]

The *Brandenburg* doctrine, however, has been subject to an increasing amount of criticism, with commentators questioning whether it is flexible enough to deal with the current threat, terrorism, and new media, particularly the Internet.[23] The thrust of this Note, however, is that *Brandenburg*'s critics might just achieve the end they seek—greater protection from allegedly threatening material on the Internet—without having to tinker with the *Brandenburg* test at all. The reason? The federal government is putting increasing pressure on Internet Service Providers, which are not bound by the constitutional rules that bind government action, to censor questionable online material.[24]

This Note will argue that the *Brandenburg* test, a robust protection for free speech developed through decades of turmoil, is in serious danger of sliding into obsolescence because of the government's ability to pressure private companies into scrubbing their networks of speech that should be protected. Part II of this Note presents a history of the Court's jurisprudence leading up to *Brandenburg*, focusing primarily on the development of the "clear and present danger" doctrine, the predecessor to the *Brandenburg* test.

---

[21] *See infra* Part V.B.2; *see also* David G. Savage, *Simple Phrase Was Key to Case; A Provision Making It a Crime To 'Provide Material Support' To Terrorists Was Crucial To the Prosecution of Padilla*, L.A. TIMES, Aug. 17, 2007, at A29.

[22] 395 U.S. 444, 447 (1969).

[23] *See, e.g.*, Margulies, *supra* note 10, at 33–38; Thomas E. Crocco, Comment, *Inciting Terrorism on the Internet: An Application of Brandenburg to Terrorist Websites*, 23 ST. LOUIS U. PUB. L. REV. 451, 457–58 (2004); John P. Cronan, *The Next Challenge for the First Amendment: The Framework for an Internet Incitement Standard*, 51 CATH. U. L. REV. 425, 428 (2002); Scott Hammock, *The Internet Loophole: Why Threatening Speech On-Line Requires a Modification of the Courts' Approach to True Threats and Incitement*, 36 COLUM. J.L. & SOC. PROBS. 65, 67 (2002); Holly S. Hawkins, Note, *A Sliding Scale Approach for Evaluating the Terrorist Threat Over the Internet*, 73 GEO. WASH. L. REV. 633, 633–34 (2004); Robert S. Tanenbaum, Comment, *Preaching Terror: Free Speech or Wartime Incitement?*, 55 AM. U. L. REV. 785, 790 (2006); Alexander Tsesis, *Prohibiting Incitement on the Internet*, 7 VA. J.L. & TECH. 5, ¶¶ 3–4 (2002), http://www.vjolt.net/vol7/issue2/v7i2_a05-Tsesis.pdf.

[24] *See, e.g.*, Seth F. Kreimer, *Censorship By Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 11, 14 (2006) ("Rather than attacking speakers or listeners directly, governments have sought to enlist private actors within the chain as proxy censors to control the flow of information.").

Part III examines the Court's decision in *Brandenburg*, and the application of the doctrine in subsequent cases. Part IV assesses the current threat level facing the country and considers criticism of the *Brandenburg* test, particularly regarding its application to speech on the Internet. Part V examines recent cases and situations that showcase government attempts to control information on the Internet. Part VI recommends ways to limit government control. It is an understatement to say that President Obama has a full plate at the start of his presidency. The economic crisis will surely dominate much of his legislative agenda for the near future. It is this author's hope, however, that he will also move quickly to reverse some of the overreaching in the anti-terrorism arena that occurred during the Bush years.

II. THE DEVELOPMENT OF THE CLEAR AND PRESENT DANGER DOCTRINE

The path from the Court's incitement jurisprudence at the turn of the twentieth century to *Brandenburg* is a long and difficult one; it is also a well-traveled one in academic literature. Nevertheless, it is critical in any analysis of *Brandenburg* to describe, at least briefly, the development of the law that informed the Court's decision in 1969.

A. *World War I Cases*

1. Schenck v. United States

Schenck was the general secretary of the Socialist Party in the United States and was convicted of conspiring to violate the Espionage Act of 1917.[25] He ordered the printing of 15,000 leaflets critical of the U.S. war effort and planned to send some of those leaflets to men who had been drafted and distribute the rest.[26] Justice Holmes, writing for the Court, introduced the clear and present danger doctrine:

> The question in every case is whether the words used are used in such circumstances and are of such a nature as to create a clear and present

---

[25] Schenck v. United States, 249 U.S. 47, 48–49 (1919).

[26] *Id.* at 49–50. The first side of the leaflet contained the first section of the Thirteenth Amendment, argued that the federal Conscription Act was a "monstrous wrong against humanity," and urged recipients to "petition for the repeal of the act." *Id.* at 50–51. The other side of the leaflet maintained that pro-war arguments were coming from "cunning politicians and a mercenary capitalist press" and argued that people violated the Constitution when they failed to assert their opposition to the draft. *Id.* at 51.

> danger that they will bring about the substantive evils that Congress has a right to prevent. It is a question of proximity and degree.[27]

For Holmes, the fact that the nation was at war was critical. In times of war, he wrote, "many things that might be said in time of peace are such a hindrance to its effort that their utterance will not be endured so long as men fight and that no Court could regard them as protected by any constitutional right."[28] The Court affirmed the convictions.

2. Frohwerk v. United States

Frohwerk and Gleeser were convicted under the Espionage Act of 1917 for helping prepare and publish a series of articles in the German-language *Missouri Staats Zeitung* that criticized the war effort and the government's draft policies.[29] Holmes, again writing for the Court, relied on the reasoning in *Schenck*, which the Court had decided just a week before:

> It may be that all this might be said or written even in time of war in circumstances that would not make it a crime. . . . [But] we must take the case on the record as it is, and on the record it is impossible to say that it might not have been found that the circulation of the paper was in quarters where a little breath would be enough to kindle a flame and that the fact was known and relied upon by those who sent the paper out.[30]

The Court unanimously rejected Frohwerk and Gleeser's First Amendment arguments and affirmed their convictions.

---

[27] *Id.* at 52.

[28] *Schenck*, 249 U.S. at 52. It was also in this passage that Holmes, making the point that the context in which words are spoken help determine whether the speech is constitutionally protected, famously wrote: "The most stringent protection of free speech would not protect a man in falsely shouting fire in a theatre and causing a panic." *Id.*

[29] Frohwerk v. United States, 249 U.S. 204, 205, 207–08 (1919). The first article "declar[ed] it a monumental and inexcusable mistake to send our soldiers to France [and] that it appears to be outright murder without serving anything practical." *Id.* at 207. A subsequent article told the story of a drafted man realizing that the war was only being fought to "protect some rich men's money" and concluded, "[w]ho then . . . will pronounce a verdict of guilty upon him if he stops reasoning and follows the first impulse of nature: self-preservation." *Id.* at 207–08.

[30] *Id.* at 208–09. The chances of the First Amendment arguments carrying the day appeared dim when Holmes began this way: "We venture to believe that neither Hamilton nor Madison, nor any other competent person then or later, ever supposed that to make criminal the counselling of a murder within the jurisdiction of Congress would be an unconstitutional interference with free speech." *Id.* at 206.

3. Debs v. United States

Eugene V. Debs, national leader of the Socialist Party, was convicted of violating the Espionage Act of 1917 for giving a speech in Canton, Ohio, that predicted the continued growth and ultimate success of Socialism, and praised the efforts of multiple individuals who had helped others resist the draft.[31] The Court decided the case on the same day as *Frohwerk*, with Holmes again writing for the majority. Holmes reasoned that the Court had "disposed of" Debs's First Amendment arguments in *Schenck*.[32] Holmes conceded that the speech would have been protected if it had only been about Socialism.[33] But if Debs intended to obstruct the war effort and if that would be the speech's "probable effect," it would not be protected.[34] The Court unanimously affirmed the conviction.

4. Abrams v. United States

Five Russian-born immigrants were convicted under the Espionage Act, which Congress had amended to include even stricter provisions on speech critical of the war effort in 1918, for printing and distributing 5,000 leaflets denouncing the United States and its allies and President Wilson, and praising the Russian revolution.[35] Justice Clark, writing for the Court, noted that the Court had "sufficiently discussed" and rejected the defendants' First Amendment argument in *Schenck* and *Frohwerk*, and affirmed the convictions.[36]

Abrams, however, broke the unanimity of the Court in cases involving convictions under the Espionage Act. Holmes, who wrote the opinions in *Schenck*, *Frohwerk*, and *Debs*, was now in dissent. Holmes's opinion in

---

[31] Debs v. United States, 249 U.S. 211, 212–14 (1919). Debs also made several statements about the "master class" abusing the "subject class" during times of war, including that the "working class, who furnish the corpses, have never yet had a voice in declaring war and never yet had a voice in declaring peace." *Id.* at 213–14

[32] *Id.* at 215.

[33] *Id.* at 212.

[34] *Id.* at 215. Holmes noted that the jury was "carefully instructed that they could not find the defendant guilty for advocacy of any of his opinions unless the words used had as their natural tendency and reasonably probable effect to obstruct the recruiting service . . . and unless the defendant had the specific intent to do so." *Id.* at 216.

[35] Abrams v. United States, 250 U.S. 616, 616–18, 619–20 (1919). The immigrants' anger was sparked when the United States sent a small contingent of troops into Russia as part of an operation against Germany, a move that the leafleters interpreted as an attempt to put down the revolution. *Id.* at 625.

[36] *Id.* at 619.

Abrams has become one of the most famous in First Amendment jurisprudence. He stood behind his decisions in *Schenck*, *Frohwerk*, and *Debs*, but found a significant difference in this case: the defendants did not have the intent required by the Act to "cripple or hinder the United States in the prosecution of the war."[37] There was nothing in the language of the leaflets, Holmes argued, that showed the men were specifically aiming to disrupt the war effort.[38]

But Holmes, who was joined by Justice Brandeis in dissent, said there was an even more important factor that caused him to dissent, namely, that "Congress shall make no law abridging freedom of speech."[39] And with that, he discussed his belief in what has come to be called the "marketplace of ideas" rationale for protecting speech:

> [W]hen men have realized that time has upset many fighting faiths, they may come to believe even more than they believe the very foundations of their own conduct that the ultimate good desired is better reached by free trade in ideas — that the best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out. That at any rate is the theory of our Constitution.[40]

Although Holmes was in dissent in *Abrams*, his opinion—refining the clear and present danger doctrine to include the elements of imminence and intent, and promoting a marketplace approach to speech—had enormous influence on the development of the incitement standard eventually adopted by the Court in *Brandenburg*.

B. *Post-World War I Cases*

Justices Holmes and Brandeis continued to operate at odds with the rest of the Court in incitement cases following World War I. The most common incitement cases during this period involved criminal syndicalism statutes passed at the turn of the twentieth century to deal with perceived threats from

---

[37] *Id.* at 626 (Holmes, J., dissenting).

[38] *Id.* at 626–27.

[39] *Abrams*, 250 U.S. at 627.

[40] *Id.* at 630. Holmes also backed away from his prior assertions that times of war fundamentally changed the right of free speech, writing that, "as against dangers peculiar to war, as against others, the principle of the right to free speech is always the same. It is only the present danger of immediate evil or an intent to bring it about that warrants Congress in setting a limit to the expression of opinion." *Id.* at 628.

anarchists,[41] but that were applied most commonly following the war to elements of the political left.

1. Gitlow v. New York

Gitlow was convicted for violating New York's criminal anarchy statute, which prohibited any person from "advocat[ing], advis[ing], or teach[ing] the duty, necessity or propriety of overthrowing . . . organized government by force or violence, or by assassination of [any] . . . executive officials of government, or by any unlawful means."[42] He was a member of the National Council of the Left Wing Section of the Socialist Party, a faction opposed to the party's platform of "moderate Socialism."[43] The National Council developed a militant "manifesto" published in the "Revolutionary Age, the official organ of the Left Wing."[44]Justice Sanford, writing for the Court, began his analysis by noting that New York's statute "does not penalize the utterance or publication of abstract doctrine or academic discussion having no quality of incitement to any concrete action."[45] But the manifesto, Sanford wrote, did not contain such abstract doctrine; rather, it "advocate[d] and urge[d] in fervent language mass action [that would] progressively foment industrial disturbances and through political mass strikes and revolutionary mass action overthrow and destroy organized parliamentary government."[46] Sanford reasoned, in affirming the conviction, that speech advocating the overthrow of organized government is sufficiently dangerous to allow legislatures to forbid it.[47]Justice Holmes, joined by Justice Brandeis in

---

[41] William M. Wiecek, *The Legal Foundations of Domestic Anticommunism: The Background of* Dennis v. United States, 2001 SUP. CT. REV. 375, 382, 392–93 (2001) (noting that "class conflict allied with nativism produced the earliest political effects of antiradicalism: the first wave of criminal anarchy statutes enacted in response to the Haymarket Massacre and the Great Upheaval of 1886, followed by a successor wave after the assassination of President William McKinley in 1902").

[42] Gitlow v. New York, 268 U.S. 652, 654 (1925).

[43] *Id.* at 655 (internal quotation marks omitted).

[44] *Id.* at 655–56. The manifesto advocated "the necessity of accomplishing the Communist Revolution by a militant and revolutionary Socialism, based on . . . revolutionary mass action, for the purpose of conquering and destroying the parliamentary state and establishing in its place . . . the system of Communist Socialism." *Id.* at 657–58 (internal quotation marks omitted).

[45] *Id.* at 664 (internal quotation marks omitted).

[46] *Gitlow*, 268 U.S. at 665.

[47] *Id.* at 669. Sanford wrote that the "State cannot reasonably be required to measure the danger from every such utterance in the nice balance of a jeweler's scale. A single revolutionary spark may kindle a fire that, smouldering for a time, may burst into a sweeping and destructive conflagration." *Id.*

dissent, reasoned that if the Court applied his conception of the clear and present danger test in this case, "it is manifest that there was no present danger of an attempt to overthrow the government by force on the part of the admittedly small minority who shared the defendant's views."[48] Holmes conceded that if the manifesto "had been laid as an attempt to induce an uprising against government at once and not at some indefinite time in the future it would have presented a different question."[49] But as it stood, Gitlow's indictment "allege[d] . . . publication and nothing more."[50]

2. Whitney v. California

Whitney was convicted of violating the California Criminal Syndicalism Act, which prohibited any person to "knowingly become[] a member of . . . any organization, society, group or assemblage of persons organized or assembled to advocate, teach or aid and abet criminal syndicalism."[51] She was a member of the Communist Labor Party, an offshoot of the Socialist Party that advocated more radical views, including the overthrow of capitalist rule through a working class revolution.[52] Unlike Gitlow, then, Whitney was convicted not for advocating herself the overthrow of organized government, but for knowingly being a member of an organization that did.

Justice Sanford, writing for the Court, wrote that great deference should be given to the judgment of the California legislature that becoming a member of a group advocating the overthrow of government "involves such danger to the public peace and the security of the State, that these acts should be penalized in the exercise of [the State's] police power."[53] Sanford reasoned, in affirming Whitney's conviction, that the activities prohibited by the Act amounted to criminal conspiracy and outweighed any free speech and associational rights that might be implicated.[54]

---

[48] *Id.* at 673 (Holmes, J., dissenting).

[49] *Id.*

[50] *Id.*

[51] Whitney v. California, 274 U.S. 357, 360 (1927).

[52] *Id.* at 363–64. At a convention of the Communist Labor Party in Oakland, California, Whitney sponsored a resolution that advocated using the political process to achieve the Communist agenda, but voters rejected the resolution. *Id.* at 365–66. Despite the defeat of her resolution, Whitney continued as a member of the Communist Labor Party after the convention, and continued to maintain that the party should not be "an instrument of terrorism or violence." *Id.* at 366.

[53] *Id.* at 371.

[54] *Whitney*, 274 U.S. at 371.

Justice Brandeis, joined by Justice Holmes, concurred in the result because Whitney failed to raise the First Amendment issue on appeal.[55] But that did not stop Brandeis from severely criticizing the majority's reasoning.[56] Without explicitly saying so, Brandeis made clear that he doubted that Whitney's association with the Communist Labor Party presented a clear and present danger. "The novelty in the prohibition introduced," Brandeis wrote, "is that the statute aims, not at the practice of criminal syndicalism, nor even directly at the preaching of it, but at association with those who propose to preach it."[57]

C. *The Cold War and* Dennis

Whatever hopes there may have been that the Court would adopt the Holmes-Brandeis approach to incitement cases were thoroughly dashed with the end of World War II and the advent of the Cold War. The Soviet Union represented a substantial and unprecedented threat to U.S. interests, and there was widespread suspicion in the public generally, and even on the Court itself, about the motivations and goals of American Communists.[58] The manifestation of this suspicion is on full display in *Dennis v. United States*.[59]

---

[55] *Id.* at 379 (Brandeis, J., concurring).

[56] Brandeis wrote:

> Fear of serious injury cannot alone justify suppression of free speech and assembly. Men feared witches and burnt women. It is the function of speech to free men from the bondage of irrational fears. To justify suppression of free speech there must be reasonable ground to fear that serious evil will result if free speech is practiced. There must be reasonable ground to believe that the danger apprehended is imminent. There must be reasonable ground to believe that the evil to be prevented is a serious one.

Id. at 376.

[57] *Id.* at 373.

[58] Wiecek, *supra* note 41, at 406. Wiecek notes:

> A majority of the Justices regarded Communists and their party as *sui generis*, different from other radical groups like the Klan, uniquely threatening to America's national security. The Court therefore assigned Communists a special status under the Constitution, with diminished protections for their speech, press, and associational liberties. They saw this contracted and distinctive status as necessary if federal, state, and local governments were to ensure their own survival.

Id.

[59] 341 U.S. 494 (1951).

1. Dennis v. United States

Dennis, general secretary of the Communist Party of the United States of America, and several others were convicted of violating the federal Smith Act, which prohibited "knowingly or willfully advocat[ing], abet[ting], advis[ing], or teach[ing] the duty, necessity, desirability, or propriety of overthrowing or destroying any government of the United States by force or violence, or by the assassination of any officer of such government," or attempting or conspiring to do any of the prohibited acts.[60] The indictment charged the defendants with conspiring to organize as the U.S. Communist Party, a "society, group and assembly of persons who teach and advocate the overthrow and destruction of the Government of the United States by force and violence."[61]

Chief Justice Vinson, writing for the Court, first set out to clarify the parameters of the clear and present danger doctrine. "Obviously," he wrote, "the words cannot mean that before the Government may act, it must wait until the *putsch* is about to be executed, the plans have been laid and the signal is awaited."[62] Vinson reasoned that "an attempt to overthrow the Government by force, even though doomed from the outset because of inadequate numbers or power of the revolutionists, is a sufficient evil for Congress to prevent."[63] Vinson then adopted the interpretation of the doctrine adopted below by Judge Learned Hand: "In each case [courts] must ask whether the gravity of the 'evil,' discounted by its improbability, justifies such invasion of free speech as is necessary to avoid the danger."[64] This formulation amounted to a significant watering down of the doctrine as interpreted by Holmes and Brandeis—gone were the requirements of imminence and intent—and it placed near-absolute importance on the perceived threat of Communists by the judge and jury. The Court affirmed the convictions.[65]

---

[60] *Id.* at 496–97.

[61] *Id.* at 497.

[62] *Id.* at 509.

[63] *Id.*

[64] *Id.* at 510.

[65] Vinson made clear that he considered Communism a serious threat to the United States:

> The formation by petitioners of such a highly organized conspiracy, with rigidly disciplined members subject to call when the leaders, these petitioners, felt that the time had come for action, coupled with the inflammable nature of world conditions, similar uprisings in other countries, and the touch-and-go nature of our relations with countries with whom petitioners were in the very least ideologically attuned, convince us that their convictions were justified on this score.

Justices Black and Douglas dissented. Justice Douglas openly doubted whether Communism was really a serious threat to the nation. "Communism in the world scene," he wrote, "is no bogeyman; but Communism as a political faction or party in this country plainly is. Communism has been so thoroughly exposed in this country that it has been crippled as a political force. Free speech has destroyed it as an effective political party."[66] Justice Black maintained that "the only way to affirm these convictions is to repudiate directly or indirectly the established clear and present danger rule."[67]

2. *Post*-Dennis *Decisions*

Two Supreme Court cases following *Dennis* helped pave the way for what would become the *Brandenburg* doctrine. The first was *Yates v. United States*, in which the Court overturned the convictions of fourteen individuals for conspiring to violate the Smith Act.[68] The issue for the Court was whether the Smith Act prohibited advocacy of forcible overthrow of the government, even if an individual took no affirmative steps to achieve that result.[69] The Court held that it did not. "That sort of advocacy," the Court noted, "even though uttered with the hope that it may ultimately lead to violent revolution, is too remote from concrete action to be regarded as the kind of indoctrination preparatory to action which was condemned in *Dennis*."[70] The Court reasoned that "[t]he essential distinction is that those to whom the advocacy is addressed must be urged to *do* something, now or in the future, rather than merely to *believe* in something."[71]

The other case was *Noto v. United States*, in which the Court overturned the conviction of a man for violating the clause of the Smith Act forbidding becoming a member of a group that advocated overthrow of the government.[72] The Court considered the testimony of witnesses at Noto's

---

Dennis, 341 U.S. at 510–11.

[66] *Id.* at 588 (Douglas, J., dissenting).

[67] *Id.* at 579–80 (Black, J., dissenting) (internal quotation marks omitted). Black concluded with the hope "that in calmer times, when present pressures, passions and fears subside, this or some later Court will restore the First Amendment liberties to the high preferred place where they belong in a free society." *Id.* at 581.

[68] 354 U.S. 298, 300, 338 (1957).

[69] *Id.* at 318.

[70] *Id.* at 321–22.

[71] *Id.* at 324–25.

[72] 367 U.S. 290, 291, 300 (1961). *Noto* was a companion case to Scales v. United States, 367 U.S. 203 (1961). The cases are different from *Dennis* and *Yates* because they involve membership in the Communist Party—governed by another section of the Smith

trial—which consisted primarily of general descriptions of Community Party activity in upstate New York—and concluded that the evidence had the same weaknesses as the evidence in *Yates*.[73] Recalling its reasoning in that case, the Court held that "the mere abstract teaching of Communist theory, including the teaching of the moral propriety or even moral necessity for a resort to force and violence, is not the same as preparing a group for violent action and steeling it to such action."[74] Indeed, the Court continued, "[t]here must be some substantial direct or circumstantial evidence of a call to violence now or in the future which is both sufficiently strong and sufficiently pervasive to lend color to the otherwise ambiguous theoretical material regarding Communist Party teaching."[75]

The principles of *Yates* and *Noto* are closely related but distinguishable. In *Yates*, it was the distinction between advocacy of action and advocacy of belief that drove the Court's decision.[76] In *Noto*, it was the distinction between abstract teaching and "preparing" and "steeling" others to action.[77] Both cases would play a critical role in the Court's *Brandenburg* decision.[78]

III. THE *BRANDENBURG* DOCTRINE

In a tightly packed opinion in *Brandenburg v. Ohio*, the Court swept away much of the World War I and World War II case law, adopted portions of *Noto* and *Yates*, and introduced prominent new speech protections.[79] But in large part because of *Brandenburg*'s brevity, important questions remained about the precise scope of its holding, questions that were not entirely answered by subsequent cases that applied its doctrine.

Act—rather than incitement-type speech related to party doctrine. In *Scales*, the Court held that for a conviction to stand under the Act's membership provision, an individual's membership in the Party had to be "active and purposive," and coupled with the "specific intent to bring about violent overthrow as speedily as circumstances would permit." *Id.* at 209, 220 (internal quotation marks omitted).

[73] *Noto*, 367 U.S. at 291–96.

[74] *Id.* at 297–98.

[75] *Id.* at 298.

[76] *Yates*, 354 U.S. at 322.

[77] *Noto*, 367 U.S. at 297–98.

[78] *See* Marc Rohr, *Grand Illusion: The* Brandenburg *Test and Speech That Encourages or Facilitates Criminal Acts*, 38 WILLAMETTE L. REV. 1, 5–10 (2002).

[79] 395 U.S. 444, 447–49 (1969).

A. Brandenburg v. Ohio

After a half century of incitement cases related to socialism and communism, the case that gave us the modern incitement doctrine arose from an entirely distinct set of facts. The appellant in *Brandenburg v. Ohio* was the leader of a Ku Klux Klan group in the Cincinnati, Ohio, area, and had been convicted under an Ohio criminal syndicalism law that banned advocating violence as a means of achieving political reform.[80] The appellant had invited a reporter from a Cincinnati television station to attend a Ku Klux Klan rally, and it was the reporter's two films of that rally that formed the prosecution's case.[81] The first film showed twelve hooded figures around a burning cross saying things derogatory to Blacks and Jews, as well as a speech by the appellant, in which he warned that "if our President, our Congress, our Supreme Court, continues to suppress the white, Caucasian race, it's possible that there might have to be some revengeance [sic] taken."[82] The second film showed the appellant making a similar speech, without any reference to the possibility of "revengeance."[83]

The Court, in a short per curiam opinion, noted that it had upheld the constitutionality of a statute very similar to Ohio's in *Whitney v. California*[84] on the ground that advocating violent action to achieve political and economic change was dangerous enough for the government to ban it.[85] But that decision, the Court concluded, had "been thoroughly discredited by later decisions."[86] And with that, the Court overruled *Whitney* and set out the formulation of the incitement standard that remains the law today:

> [T]he constitutional guarantees of free speech and free press do not permit a State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action.[87]

---

[80] *Brandenburg*, 395 U.S. at 444–45.

[81] *Id.* at 445.

[82] *Id.* at 445–46.

[83] *Id.* at 447.

[84] 274 U.S. 357, 359–60 (1927).

[85] *Id.*

[86] *Brandenburg*, 395 U.S. at 447 (citing Dennis v. United States, 341 U.S. 494, 507 (1951)).

[87] *Id. See also* Rohr, *supra* note 78, at 7. Professor Rohr authoritatively points out a number of the peculiarities of *Brandenburg*, including the Court's citing only *Dennis* for the notion that *Whitney* had been discredited; the somewhat nonchalant tone of the Court in formulating its new test; and the Court, in a footnote accompanying the new test, asserting that it had upheld the Smith Act in *Dennis* only because it understood the statute to have adhered to the just-formulated test. As Rohr puts it:

Two critical factors missing from previous formulations of the incitement test—"imminence" and "likelihood"—appeared to provide significantly more protection to speech that advocated lawless action.

Legitimate questions remain, however, about how much protection *Brandenburg* actually provides. The Court, for example, explicitly *did not* overrule *Dennis*, which contained the Court's last significant articulation of the clear and present danger test, and which upheld an application of the Smith Act that appears incompatible with the *Brandenburg* test.[88] Indeed, the Court did not even mention the clear and present danger test in *Brandenburg*, and—by prominently citing *Noto v. United States* and *Yates v. United States* in the same passage as its new doctrine—appeared to rely more heavily on principles of those cases distinguishing abstract advocacy or teaching from action or preparing others for action.[89] The Court concluded that "[a] statute which fails to draw this distinction impermissibly intrudes upon the freedoms guaranteed by the First and Fourteenth Amendments. It sweeps within its condemnation speech which our Constitution has immunized from governmental control."[90]

Yet, for any questions that might linger about *Brandenburg*'s scope, there is little doubt, as Professor Kalven put it, that the decision is "of great significance."[91] First, it "placed beyond censorship the 'mere advocacy' of violence," precisely the type of advocacy that had snagged so many speakers in the line of cases dating back to *Schenck v. United States*.[92] Second, it "reset the boundary line of permissible censorship" with its new "magic words": "incitement to imminent lawless action."[93] For Kalven,

---

> Something was seriously askew here. The Court had just articulated a verbal formula that appeared more protective of seditious advocacy than any statement ever before made in a Supreme Court majority opinion, yet it was simultaneously suggesting that (a) this was nothing new, and (b) it was fully consistent with a decision (*Dennis*) that had upheld the conviction of advocates of revolution without any concern for the "imminence" or "likelihood" of that revolution. Either the author of the opinion was being quite disingenuous, or the apparently highly-protective new test was not meant to provide as much protection as its words suggested.

Id. at 7–8 (internal citations omitted). For another worthwhile discussion of *Brandenburg*'s idiosyncrasies, see HARRY KALVEN, JR., A WORTHY TRADITION: FREEDOM OF SPEECH IN AMERICA 121–24, 231–34 (1988).

[88] 395 U.S. at 447–48.

[89] Rohr, *supra* note 78, at 8–9.

[90] *Brandenburg*, 395 U.S. at 447–48.

[91] KALVEN, *supra* note 87, at 123.

[92] *Id.*

[93] *Id.* at 124.

"'incitement' has the ring of a term of art and is the best word for marking the minimal jurisdiction over political speech that concern with public order requires be ceded to censorship. It marks the last term in a series."[94]

B. *Post*-Brandenburg *Decisions*

Subsequent cases have not resolved *Brandenburg*'s ambiguities. The Court "has returned to *Brandenburg* remarkably infrequently" since deciding the case in 1969,[95] although the two significant cases applying *Brandenburg* supply some additional clues as to its holding's scope. In the first, *Hess v. Indiana*, the Court, in a per curiam opinion, overturned the disorderly conduct conviction of an antiwar demonstrator who, while facing a crowd, said, "We'll take the fucking street later," or "We'll take the fucking street again."[96] "At best," the Court reasoned, "the statement could be taken as counsel for present moderation; at worst, it amounted to nothing more than advocacy of illegal action at some indefinite future time."[97] Invoking the *Brandenburg* test, the Court held that "since there was no evidence, or rational inference" that the demonstrator's "words were intended to produce, and likely to produce, *imminent* disorder, those words could not be punished by the State on the ground that they had 'a tendency to lead to violence.'"[98] The importance of the *Hess* decision is in its conception of "imminence" in the *Brandenburg* test. As Professor Rohr has noted,

> [i]t is possible to view the *Hess* decision as standing for the proposition that even in a case involving advocacy of illegal action intended to take place (and perhaps likely to take place) several hours (at most) in the future, that relatively minimal temporal relationship between speech and resulting harm

is not enough to satisfy the *Brandenburg* test.[99]

In the second case, *NAACP v. Claiborne Hardware Co.*, the Court, per Justice Stevens, reversed a state court judgment against organizers of a boycott of white-owned businesses by black residents in Claiborne County, Mississippi.[100] The Court focused especially on public speeches given by NAACP official Charles Evers, including one in particular in which he urged a total boycott of white merchants and stated: "If we catch any of you going

---

[94] *Id.*

[95] Rohr, *supra* note 78, at 10.

[96] 414 U.S. 105, 105–07, 109 (1973).

[97] *Id.* at 108.

[98] *Id.* at 109 (internal quotation marks omitted).

[99] Rohr, *supra* note 78, at 12.

[100] 458 U.S. 886, 889, 934 (1982).

in any of them racist stores, we're gonna break your damn neck."[101] The Court acknowledged that "in the passionate atmosphere in which the speeches were delivered, they might have been understood as inviting an unlawful form of discipline or, at least, as intending to create a fear of violence whether or not improper discipline was specifically intended."[102] Indeed, there was evidence of scattered acts of violence against the property of individuals who ignored the boycott.[103] But the Court held that the contents of the speech did not violate the *Brandenburg* test.[104] If Evers's "language had been followed by acts of violence, a substantial question would be presented whether Evers could be held liable for the consequences of that unlawful conduct. In this case, however . . . the acts of violence . . . occurred weeks or months after the . . . speech . . . ."[105] *Claiborne Hardware* thus stands for the proposition that the Court is willing to consider whether unlawful action actually followed speech, and not just for whether unlawful action was likely or imminent.[106]

Claiborne Hardware effectively marks the end of the line of Supreme Court cases applying the *Brandenburg* doctrine. Questions still remain about the doctrine's true meaning, particularly the scope of its "imminence" and "likelihood" requirements. But its power is evident in the absence, since the doctrine's adoption, of the types of convictions of government and war critics that were so prominent in the first half of the 20th century.

IV. THE CURRENT THREAT AND CALLS TO ALTER *BRANDENBURG*

As mentioned in the introduction, and as should be apparent after the survey of the development of the *Brandenburg* doctrine, the perceived threat level facing the country has been a critically important factor in the Court's decisions regarding speech advocating unlawful action. The fear of Communism that gripped the country for the better part of a half-century played a role in the line of regrettable decisions from *Schenck* to *Dennis*, just as the lack of fear of a Communist takeover after the worst of the Red Scare

---

[101] *Id.* at 902.

[102] *Id.* at 927.

[103] *Id.* at 904 ("[I]n two cases, shots were fired at a house; in a third, a brick was thrown through a windshield; in the fourth, a flower garden was damaged.").

[104] *Id.* at 928.

[105] *Id.*

[106] *See* Rohr, *supra* note 78, at 14. Rohr considers Court's use of *Brandenburg* "somewhat perplexing." *Id.* "Still," he continues, "it was employed in the service of freedom of speech, and, ultimately, the fact that this case was all about a civil suit for damages may explain Stevens' apparent requirement of a link between the speech and a resulting act of violence." *Id.*

played a role in the speech-protective decisions of *Brandenburg*, *Hess*, and *Claiborne Hardware*.

Compared with the cloud of fear that hung over the country in the months following 9/11, there is little doubt that the situation today is fundamentally different. It was natural for the nation to defensively recoil from 9/11 and, in the immediate aftermath, to try to do anything and everything possible to prevent additional attacks. But with so many years passing without any more attacks, and with no demonstrable evidence of a growing terrorist threat within our borders, it is not a stretch to argue that the threat is largely contained.[107] Moreover, the plots the government has uncovered make the threat of another large-scale attack seem remote indeed.

There were the so-called "Lackawanna Six," a group of Arab Americans in their twenties who traveled from Lackawanna, N.Y., to an al-Qaeda camp in Afghanistan in early 2001, returning prior to 9/11.[108] They were arrested in September 2002, within days of the first anniversary of 9/11, and branded variously as "the enemy within," an "al-Qaeda sleeper cell," and traitors who had known about the 9/11 plot and failed to warn authorities.[109] But not only did the men not know about the 9/11 plot, they were so uncomfortable with their presence in the al-Qaeda camp that they faked injuries and came home early, eager to "put their brush with Islamic extremism behind them."[110] At the time of their arrests, none of the Lackawanna Six had signed the jihadist's pledge of loyalty to Osama bin Laden, the mastermind of the 9/11 attacks, and none appeared to be actively plotting attacks within the United States.[111] The men all eventually pleaded guilty to providing material support to al-Qaeda, receiving sentences ranging from seven to nine years.[112]

There were the so-called "Liberty City Seven," a group of struggling construction workers in Miami, Fla., who the government said wanted to join forces with al-Qaeda in attacks on the Sears Tower in Chicago.[113] Then-Attorney General Alberto Gonzales described the men as typical of "smaller, more loosely defined cells who are . . . inspired by a violent jihadist

---

[107] *See supra* notes 5 and 6 and accompanying text.

[108] Dina Temple-Raston, *The Enemy Within? Not Quite*, WASH. POST, Sept. 9, 2007, at B1.

[109] *Id.*

[110] *Id.*

[111] *Id.*

[112] *Id.*

[113] Vanessa Blum, *Jurors Wanted Terrorism Proof; Four Firmly Against Any Convictions, Skeptical About Liberty Seven's Intent*, SUN-SENTINEL, Dec. 15, 2007, at 1B.

message."[114] Some defense attorneys and media accounts, on the other hand, described the men "as a group of ragtag wannabes who could never carry out the large-scale violence they were charged with plotting."[115] Officials acknowledged that the men "had never acquired weapons or equipment and had posed no immediate threat."[116] One of the seven was ultimately acquitted, and a mistrial was declared in the case of the six others when the jury deadlocked.[117]

There were the six foreign-born "radical Islamists" arrested and indicted in May 2007 after they attempted to buy weapons from an FBI informant as part of an alleged plot to attack Fort Dix in New Jersey.[118] The FBI started investigating the group after one of the suspects took a videotape to a store to have it copied onto a DVD.[119] The video depicted the men firing assault rifles and yelling in Arabic.[120] A successful attack on the heavily fortified base is considered "highly unlikely."[121] And the fact that the men got caught by taking their highly suspicious video to a store for copying "'somewhat indicates they weren't the A-team of terrorists.'"[122] Five of the six men were ultimately convicted of conspiring to kill U.S. soldiers, and the sixth pleaded guilty to weapons charges.[123]

And there were the four men arrested and indicted a month later for an alleged plot to blow up fuel tanks and pipelines underneath John F. Kennedy

---

[114] Alberto Gonzales, Attorney General, Press Conference at the Department of Justice (June 23, 2006), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/06/23/AR2006062300942.html.

[115] Meg Laughlin, *Terror Trial Falters Again*, ST. PETERSBURG TIMES, Dec. 14, 2007, at 1A.

[116] Kirk Semple, *U.S. Falters in Terror Case Against 7 in Miami*, N.Y. TIMES, Dec. 14, 2007, at A28.

[117] Laughlin, *supra* note 115, at 1A ("With no guilty verdicts, the Liberty City Seven join about a dozen other terrorism defendants around the country who have been prosecuted since the Sept. 11 attacks in costly cases that resulted in acquittals and mistrials.").

[118] Josh Meyer & Erika Hayasaki, *6 Charged in Plot To Strike Army Base; The FBI Says the 'Radical Islamists' Wanted To 'Shoot Up' Ft. Dix in New Jersey*, L.A. TIMES, May 9, 2007, at A1.

[119] *Id.*

[120] *Id.*

[121] John Shiffman, *6 Held in Alleged Plot Against Base; FBI: Ft. Dix, N.J., Targeted by Suspects*, CHI. TRIB., May 9, 2007, at 18.

[122] *Id.* (quoting Daniel Benjamin, a terrorism expert and senior fellow at the Brookings Institution in Washington).

[123] William Branigin, *5 Men Convicted in Plot to Kill Soldiers at Fort Dix*, WASH. POST, Dec. 23, 2008, at A2.

International Airport in New York.[124] The purported mastermind of the attack was a 63-year-old retired airport cargo worker.[125] The plot was in such an early stage at the time of the arrests that "no plan had developed for acquiring explosives, let alone gaining access to the tanks and pipelines."[126] The men were short on cash, had never planned or carried out any previous attacks, and did not have relevant military training for the elaborate plan.[127] The New York City Police Commissioner called the retired cargo worker "a 'self-radicalized New Yorker' who was 'plotting to betray his adopted country with a catastrophic attack.'"[128] But a federal law enforcement official said the worker "seemed more like a 'sad old guy who's got a lot of spit and vinegar in him.'"[129]

The ragtag nature of the groups caught by the government so far has done little to quell the voices of those who perceive an ever-growing terrorist threat. The Internet, in particular, has emerged as a focal point for groups and commentators concerned about the country's vulnerability to future attacks. A New York City Police Department report on radicalization in the West released last year maintained that "the Internet provides the wandering mind of the conflicted young Muslim or potential convert with direct access to unfiltered radical and extremist ideology" and "serves as an anonymous virtual meeting place."[130] Once someone adopts a jihadi point of view, the report continues, the Internet, "[c]loaked with a veil of objectivity," enables the "aspiring jihadist to view the world and global conflicts through this extremist lens, further reinforcing the objectives and political arguments of the jihadi . . . agenda."[131] Similarly, a National Intelligence Estimate in 2006

---

[124] Greg Miller & Erika Hayaski, *Arrests Made in Alleged JFK Plot; Officials Say Extremists from Guyana and Trinidad Planned To Cripple the Key Airport; One Is a U.S. Citizen*, L.A. TIMES, June 3, 2007, at A1.

[125] *Id.*

[126] *Id.*

[127] Michael Powell & William K. Rashbaum, *Plot Suspects Described as Short on Cash and a Long Way from Realizing Goals*, N.Y. TIMES, June 4, 2007, at B1.

[128] Miller & Hayaski, *supra* note 124, at A1.

[129] *Id.*

[130] SILBER & BHATT, *supra* note 6, at 8; *see also* Robert M. Chesney, *Beyond Conspiracy? Anticipatory Prosecution and the Challenge of Unaffiliated Terrorism*, 80 S. CAL. L. REV. 425, 439–40 (2007) ("Ideology can be spread and inflamed on a global scale with relative ease through the online posting of various media. . . . Advice and expertise on technical issues ranging from online security to the construction of improvised explosive devices are just a click away.").

[131] SILBER & BHATT, *supra* note 6, at 8–9. Once an individual fully commits to jihad, the report concludes, "the Internet serves as an enabler—providing broad access to an array of information on targets, their vulnerabilities and the design of weapons." *Id.*

found that the "radicalization process is occurring more quickly, more widely, and more anonymously in the Internet age, raising the likelihood of surprise attacks by unknown groups whose members and supporters may be difficult to pinpoint."[132]

A report by the Anti-Defamation League in 2002 outlined many of the features of the Internet that raise concerns about its use in furthering terrorist plans.[133] Terrorists use encryption to scramble messages to one another, disseminate "secret statements embedded in apparently harmless information that is posted publicly online," or simply talk openly about upcoming plans by taking advantage of the anonymity that the Internet provides.[134] Apart from the Internet's use as a forum to plan attacks and other operations, it has also proved, as the report chronicles, an invaluable terrorist propaganda tool.[135] Al-Qaeda and other militant groups use networks of sympathetic Web sites to transmit messages from their leaders and generally promote the militant cause.[136]

Despite the fact that the vast majority of content for militant Web sites is created outside of the United States, and that the Web sites themselves are also predominantly created and hosted elsewhere,[137] many commentators have started arguing that the *Brandenburg* test is incapable of handling the new communications framework presented by the Internet.[138] Some note the

---

[132] Press Release, *supra* note 13 (concluding "groups of all stripes will increasingly use the Internet to communicate, propagandize, recruit, train, and obtain logistical and financial support").

[133] ANTI-DEFAMATION LEAGUE, JIHAD ONLINE: ISLAMIC TERRORISTS AND THE INTERNET (2002), http://www.adl.org/internet/jihad_online.pdf. The report argues that because Islamic militants "are global, rather than being located in a single geographical area, and because their message is an important tool for recruitment and incitement to violence, the Internet provides them with a new and effective way to attain their goals." *Id.* at 3; *see also* Clive Walker, *Cyber-Terrorism: Legal Principle and Law in the United Kingdom*, 110 PENN ST. L. REV. 625, 636–40 (2006) (noting terrorists' increasing usage of the Internet for communications, personnel and logistical support, intelligence gathering, and propaganda).

[134] ANTI-DEFAMATION LEAGUE, *supra* note 133, at 10–11; *see also* John D. Podesta & Raj Goyle, *Lost in Cyberspace? Finding American Liberties in a Dangerous Digital World*, 23 YALE L. & POL'Y REV. 509, 517–18 (2005) (noting that "in just the last eight years, the number of websites sponsored by terrorists has increased from a dozen to 4350, and new tools for encrypting messages are used nearly every day") (citation omitted).

[135] ANTI-DEFAMATION LEAGUE, *supra* note 133, at 12–14.

[136] *Id.*

[137] Benjamin R. Davis, *Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for Cyber Governance*, 15 COMMLAW CONSPECTUS 119, 131–35 (2006).

[138] *See supra* note 23.

simultaneous nature and lack of mediation involved in Internet communication, which effectively allows terrorists to communicate across the globe with one another, and to do so without another party—i.e., an editor or other controller of media—having any control over their communication.[139] Others note that the Internet creates a new speaker-audience relationship not contemplated by the Court that fashioned *Brandenburg*.[140] Recommendations for updating the *Brandenburg* doctrine so that it can effectively confront the current threat include expanding the relatively strict temporal requirements of the doctrine's imminence requirement[141] and placing Web sites into different categories that receive different levels of constitutional protection based on the type of information they contain.[142]

Those arguments have some merit. The terrorist threat manifested itself in attacks in this country the likes of which we have never experienced. And the Internet has undoubtedly revolutionized the way we communicate, providing instantaneous access to people and information around the world. However, the argument that the *Brandenburg* doctrine needs changing misses the essential fact that *Brandenburg* is already being weakened without any need to alter the doctrine itself.

V. CENSORSHIP BY PROXY AND *BRANDENBURG*'S DECLINE

Professor Kreimer cogently described the "First Amendment drama" as appearing in dyads: "in free speech narratives, a speaker exhorts a listener; in free press accounts, a publisher distributes literature to readers. In the usual plot, the government seeks to disrupt this dyad (for legitimate or illegitimate reasons) by focusing sanctions on the source of the speech" and, occasionally, on the listener.[143] But "the Internet . . . 'alters the drama,'" because online, "[s]peakers can hide their identities, impeding direct coercion [and] they can extend the reach of their communications into foreign jurisdictions that may face legal or practical impediments to exerting control."[144] And on the "listeners' side, an expanding universe of seekers of forbidden content can obtain access to material in private without leaving their homes, bypassing both formal and informal obstacles, and can pursue

---

[139] Margulies, *supra* note 10, at 33–36.

[140] Cronan, *supra* note 23, at 428.

[141] *Id.* at 456; Crocco, *supra* note 23, at 457–58.

[142] Hawkins, *supra* note 23, at 634.

[143] Kreimer, *supra* note 24, at 13 (internal citations omitted).

[144] *Id.*

alternative pathways when a particular route is blocked."[145] Kreimer continued:

> Faced with these challenges, state actors who seek to control Internet communications have begun to explore strategies that target neither speakers nor listeners. Regulators have fallen back on alternatives predicated on the fact that, in contrast to the usual free expression drama, the Internet is not dyadic. The Internet's resistance to direct regulation of speakers and listeners rests on a complex chain of connections, and emerging regulatory mechanisms have begun to focus on the weak links in that chain. Rather than attacking speakers or listeners directly, governments have sought to enlist private actors within the chain as proxy censors to control the flow of information.[146]

Some commentators favorably view these developments.[147] They argue that governments should actively encourage, if not require, Internet intermediaries such as Internet Service Providers ("ISPs"),[148] credit card companies,[149] and online auction sites[150] to monitor their customer traffic for

---

[145] *Id.* at 13–14.

[146] *Id.* at 14.

[147] *See generally* Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003 (2001); Ronald J. Mann & Seth R. Belzley, *The Promise of Internet Intermediary Liability*, 47 WM. & MARY L. REV. 239 (2005); Joel R. Reidenberg, *Technology and Internet Jurisdiction*, 153 U. PA. L. REV. 1951 (2005); Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653 (2003).

[148] Mann & Belzley, *supra* note 147, at 255–56. ISPs play three distinct roles in Internet transactions: (1) so-called "backbone providers" operate solely at the transmission level, offering the infrastructure that makes online data transfers possible; (2) "destination ISPs" serve end users who request content over the Internet, providing a gateway to all of the information on the Web; and (3) "source ISPs" provide Internet access to individuals and businesses that create or shepherd content that is then transmitted to destination ISPs and end users. *Id. See also* Zittrain, *supra* note 147, at 656–57 ("Most ISPs themselves have ISPs—smaller ISPs can either be resellers of a larger ISP's service or simply have one or more 'transit' arrangements by which other ISPs agree to pass [information] back and forth to the smaller ISP and its customers.").

[149] Mann & Belzley, *supra* note 147, at 257–58. Credit cards, issued by a small number of dominant financial institutions that governments could target for closer regulation, are usually necessary to conduct consumer transactions online. *Id.* Person-to-person payment systems, such as PayPal, are growing in popularity and have, like credit cards, become highly concentrated in the hands of a few dominant companies that governments could easily target. *Id.*at 258. *See also* Katyal, *supra* note 147, at 1101 (noting that credit cards "are the predominant method of payment" in online criminal transactions).

[150] Mann & Belzley, *supra* note 147, at 258–59. Auction intermediaries facilitate consumer transactions between remote buyers and sellers. *Id.* at 258. EBay is the

potentially illegal activity and either investigate and terminate such activities themselves, or refer the activity to appropriate governmental authorities. Online activities that typically involve payment and auction intermediaries, such as purchasing pirated copyrighted materials and counterfeit goods, are outside the scope of this Note. The following analysis, therefore, focuses on the role of ISPs in policing online speech.

There are a handful of common suggestions for the types of actions ISPs can take to monitor not just questionable speech, but any kind of potentially illegal online activity: (1) they can "chaperone subscribers by monitoring their conduct"; (2) they can "bounce risky subscribers by purging them from the network altogether"; (3) they can "act as whistleblowers and report instances of computer crime"; (4) they can "build hardware and software constraints into their systems" that could automatically monitor and prevent illegal activity; and (5) they can adopt "methods that make it easier for law enforcement to investigate" illegal online activity, such as preserving data for long periods of time.[151] The justification for turning ISPs into de facto Internet police is that they are the least cost avoiders in the fight against online crime.[152] It is simply easier and cheaper for ISPs—with constant access to their networks and the ability to identify anonymous users in many instances—to monitor online activity than for the government to try to do so.[153]

Kreimer, on the other hand, takes a "jaundiced view of these developments," as does the author of this Note.[154] Importantly, the notion of ISPs operating as proxy censors for the government has moved beyond the realm of mere possibility to reality.[155] As one commentator has observed, the government is increasingly recruiting companies, including ISPs, to serve its national security interests, resulting in a so-called "Invisible Handshake" between the public and private sectors.[156] The dangers of this arrangement are profound. Censorship by ISPs occurs without the due process guarantees

---

dominant player in the online auction industry and is "the target of most complaints about failure to act to prevent the auction of illegal goods," making it, in turn, a logical target of those who favor greater regulation of the Internet. *Id* at 258–59.

[151] Katyal, *supra* note 147, at 1096–97.

[152] *See* Mann & Belzley, *supra* note 147, at 240; Katyal, *supra* note 147, at 1095–96.

[153] Mann & Belzley, *supra* note 147, at 268.

[154] Kreimer, *supra* note 24, at 15.

[155] *See infra* Parts V.B.1–3.

[156] Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VA. J.L. & TECH. 6, ¶¶ 2, 72 (2003), *available at* http://www.vjolt.net/vol8/issue2/v8i2_a06-Birnhack-Elkin-Koren.pdf.

that accompany government censorship.[157] ISPs are more likely to engage in "prophylactic self-censorship" because it could simply be too costly to distinguish between protected and unprotected speech.[158] Even if ISPs take the time to identify unprotected speech, they are still more likely to censor protected speech to reduce the risk of liability.[159] And ISPs are less likely to challenge efforts to censor particular speech than are the speakers themselves.[160] Against a backdrop of government encouragements and threats to ISPs, the *Brandenburg* doctrine is in jeopardy.

A. *Sami Omar Al-Hussayen and a Failed Direct Attack on Internet Speech*

A major reason why the government is leaning on the private sector to police online activity is that the *Brandenburg* doctrine makes it so difficult to secure prosecutions for inflammatory rhetoric. For example, in one of the most high-profile speech-related cases following 9/11, a federal jury in Idaho acquitted a Saudi computer student the government had accused of spreading terrorism on the Internet.[161]

Sami Omar Al-Hussayen came to the United States in 1994, studying computer science at universities in Indiana and Texas before transferring to the University of Idaho in 1999 to pursue a doctorate in computer network security.[162] It was there, the government alleged, that Al-Hussayen started using his computer skills to aid a worldwide jihadist network.[163] By day, the government argued, Hussayen was a "studious family man, but his 'private face' was that of a man who promoted 'extreme jihad' and 'provided

---

[157] Kreimer, *supra* note 24, at 27–33.

[158] *Id.* at 28 ("In networked environments, revenue from the marginal customer brings only a small payoff, a benefit that can easily be dwarfed by threatened penalties—or even by the threat of official displeasure. It is almost always cheaper to drop a marginal website than to employ counsel.").

[159] *Id.* at 30.

[160] *Id.* at 31 ("Given the divergence between their interest and those of the speakers, intermediaries are unlikely to expend much time or energy contesting dubious demands that can be satisfied by sacrificing a marginal user of their services.").

[161] *See, e.g.*, Richard B. Schmitt, *Acquittal in Terrorism Case Is a Defeat for Patriot Act*, L.A. TIMES, June 11, 2004, at A20; Susan Schmidt, *Saudi Acquitted of Internet Terror; Defense Hails Verdict on Islamic Sites as Victory for Free Speech*, WASH. POST, June 11, 2004, at A3.

[162] Les Zaitz, *Idaho Trial Explores Web's Role in Terrorism*, OREGONIAN, Apr. 12, 2004, at A1.

[163] *Id.*

recruitment and funding for terrorism'."[164] Specifically, the government charged Al-Hussayen with three counts of providing "material support" to terrorists[165] and eleven counts of false statements and visa fraud.[166] The government alleged that Al-Hussayen managed Web sites for the Islamic Assembly of North America, a non-profit charity based in Ann Arbor, Michigan, that the government suspects of supporting terrorism, and the Al-Haramain Islamic Foundation, a charity based in Saudi Arabia that the government has designated a terrorist group.[167] Through those sites, the government claimed, Al-Hussayen "published or broadcasted a wide variety of speeches, lectures and articles justifying and glorifying violent jihad, as well as graphic videos depicting mujahideen and other subjects relating to violent jihad, with the intent to inspire viewers to engage in and provide financial support for violent jihad."[168]

The trial lasted seven weeks and was taken up almost entirely by the prosecution's case, including testimony from a convicted terrorist who said he was influenced by Al-Hussayen's Web postings.[169] The crux of the government's argument was that providing such inflammatory content to aspiring jihadists was the equivalent of "providing a gun to an armed

---

[164] Susan Schmidt, *Saudi Student's Trial Opens in Idaho; Government Alleges 'Material Support' for Terrorism in Use of Internet*, WASH. POST, Apr. 15, 2004, at A5. The importance of the case to the federal government was underscored by statements made by then-Attorney General John Ashcroft, who said that "the indictment against Al-Hussayen was evidence that the Justice Department was aggressively pursuing 'those who use their specialized computer skills to knowingly and intentionally support . . . terrorist conspiracies.'" Richard B. Schmitt, *Free Speech Crux of Terrorism Case; Sami Omar Al-Hussayen's Lawyers Say He Was Trying to Foster Dialogue on His Fatwa-Filled Websites*, L.A. TIMES, May 23, 2004, at A25.

[165] For a discussion of the federal government's material-support provision, see *infra* Part V.B.2.

[166] Second Superseding Indictment, United States v. Al-Hussayen, No. CR-03-OU48-C-EJL, 14–24 (D. Idaho Mar. 12, 2004).

[167] *Id.* at 3–4.

[168] *Id.* at 6. Among the items allegedly published or maintained by Al-Hussayen were numerous articles praising jihad and martyrdom, several fatwas "justifying and encouraging violent jihad, including suicide attacks," and an e-mail group providing news about Islamic fighters in Chechnya that featured a series of postings exhorting readers to take up arms against their oppressors. *Id.* at 7, 9–10. For a concise overview of the government's case against Al-Hussayen, see Les Zaitz, *The Case of Sami Omar Al-Hussayen*, OREGONIAN, Apr. 12, 2004, at A6.

[169] Schmitt, *supra* note 161. Ahmed Bilal, the convicted terrorist, was a member of the so-called Portland Seven, an Oregon group that "tried to reach Afghanistan to fight U.S. forces in late 2001." Les Zaitz, *Convicted Jihadist To Testify in Saudi Student's Trial*, OREGONIAN, Apr. 15, 2004, at C9.

robber."[170] The defense was so confident in its case that it presented only one witness, a former CIA operative who questioned whether Internet content is capable of motivating people to become jihadists.[171] After deliberating for a week, the jury acquitted Al-Hussayen on the three counts of providing material support to terrorists and three of the visa-fraud and false-statement counts, and deadlocked on the remaining eight charges.[172] The jury concluded that Al-Hussayen's postings did not satisfy *Brandenburg*'s imminence requirement, i.e., they were not likely to produce imminent lawless action.[173] The case was a significant defeat for the government from a legal standpoint, but the Justice Department still succeeded in silencing Al-Hussayen. Besides keeping him jailed from the time of his arrest in February 2003 through his acquittal on the terrorism charges in June 2004, the government agreed to drop all remaining charges against Al-Hussayen in return for his dropping an appeal of a deportation order.[174] The government released Al-Hussayen from jail in July 2004 and immediately deported him to Saudi Arabia.[175]

B. *Pressuring ISPs to Police Online Speech*

Because of the difficulty of securing convictions against online speakers, as the Al-Hussayen case illustrates, the federal government is increasingly pressuring ISPs to control the speech of their users. The pressure is primarily applied in three ways: (1) through so-called "good corporate citizen" programs and provisions that request ISPs to voluntarily remove questionable content or alert government authorities to its existence;[176] (2) through vague provisions in the laws prohibiting material support of terrorists that create doubt about the scope of illegal speech and conduct;[177] and (3) through overuse of National Security Letters that require ISPs to turn over user

---

[170] Timothy Egan, *Computer Student on Trial Over Muslim Web Site Work*, N.Y. TIMES, Apr. 27, 2005, at A16.

[171] Schmitt, *supra* note 161.

[172] Schmidt, *supra* note 164.

[173] *Id.* In an interview after the case, one of the jurors said the jury concluded that "you can print material that advocates illegal action [and] if by printing it doesn't cause people to take imminent action, you are protected." *Id.*

[174] Bob Flick, *Feds Drop Charges Against Saudi Web Expert*, GRAND RAPIDS PRESS, July 1, 2004, at A11.

[175] *Saudi Acquitted in Terror Case Is Deported*, L.A. TIMES, July 22, 2004, at A14.

[176] *See infra* Parts V.B.1.a–b.

[177] *See infra* Part V.B.2.

information to the Federal Bureau of Investigation.[178] This Note next examines each tactic.

1. *"Good Corporate Citizen" Programs and Provisions*

a. *Government Requests to Remove Online Content*

The intense pressure that the government can apply to ISPs to get them to remove online content was on vivid display in the Second Circuit case of *Zieper v. Metzinger*.[179] In October 1999, Michael Zieper, a performance artist and filmmaker living in New Jersey, placed a short film on his Web site titled, "Military Takeover of New York City."[180] The film consisted entirely of daytime street footage of Times Square in New York City, with an off-camera narrator, purporting to be a military officer, describing plans for a military takeover of Times Square on New Year's Eve 1999.[181] The film contained no credits, titles or other markers indicating it was a work of fiction.[182] Zieper said the purpose of the film, among other things, was to explore the paranoia he believed was gripping the country before the end of the millennium.[183]

In early November 1999, the New York Police Department (NYPD) faxed information about Zieper's film to the Federal Bureau of

---

[178] *See infra* Part V.B.3.

[179] 474 F.3d 60 (2d Cir. 2007).

[180] *Id.* at 63.

[181] Brief for Plaintiffs-Appellants at 5, Zieper v. Metzinger, 474 F.3d 60 (2d Cir. 2007) (No. 05-5250-CV), 2006 WL 4663834. The site included this text as an introduction:

> Is there going to be a Military Takeover of New York City on New Year's Eve 1999? I don't know too much about this tape you are about to see. I got it from my cousin Steve who's in the army. He said that copies of this tape are floating around the base, and nobody knows who made it. If it's fake, then there's nothing to worry about. If it's real, then we're in big trouble.

Id. at 4.

[182] *Id.* (noting that Zieper "frequently employs this technique, in the tradition of War of the Worlds and The Blair Witch Project, to provoke additional thought by the viewer"); *see also* Ann Hornaday, *For Hoaxes, Mike Z Marks the Spot; 'Post-Ironic' Filmmaker Keeps It Unreal*, WASH. POST, May 11, 2003, at N1 (noting that most of Zieper's films "are so deadpan that they are more likely to leave audiences unsettled, confused or even frightened").

[183] Brief for Plaintiffs-Appellants, *supra* note 181, at 7; *see also* Mark Boal, *FBI's Shutter Speed*, VILLAGE VOICE, Nov. 30, 1999, at 38; C.J. Chivers, *Filmmaker Says U.S. Suppressed His Work*, N.Y. TIMES, Dec. 23, 1999, at B5.

Investigation's Joint Terrorism Task Force.[184] The FBI's initial investigation revealed that Zieper was the owner/operator of his Web site, and that the site was hosted by BECamation, a small Michigan company owned by Mark Wieger.[185] Wieger rented his Internet space from Online Marketing, LLC, which in turn rented its Internet space from GTE Internetworking.[186] On November, 9, 1999, the U.S. Attorney's Office for the Southern District of New York subpoenaed GTE to obtain information about Zieper's Web site.[187] At the same time, then co-chief of the Southern District of New York's Organized Crime and Terrorism Unit Patrick Fitzgerald determined that the film constituted protected speech and that the government could not order anyone to remove it from the Internet.[188] The most the government could do, Fitzgerald reasoned, was request the film's removal.[189]

The following day, FBI agent Joseph Metzinger, two NYPD officers, and an officer from the West Caldwell, New Jersey, Police Department visited Zieper's home.[190] Zieper was not at home when they arrived, but Metzinger was able to reach Zieper by phone.[191] Metzinger told Zieper that the film "might upset people who were coming to New York and that it would have a negative effect on people's plans and local businesses," and he asked if the FBI could prevent people from viewing the film.[192] Zieper said he did not think that was possible, and the two ended their conversation.[193] The next day, Zieper had his attorneys return another call from Metzinger. During that conversation, the attorneys told Metzinger that he was violating Zieper's

---

[184] *Zieper*, 474 F.3d at 63.

[185] Brief for Plaintiffs-Appellants, *supra* note 181, at 5–6. Zieper named his Web site www.crowdedtheater.com and provided a contact email address of fire@crowdedtheater.com, both in reference to Justice Holmes's famous statement in *Schenck v. United States*. *See supra* note 30 and accompanying text. The movie is still available for viewing. CrowdedTheater.com, Military Takeover of Times Square, http://www.crowdedtheater.com/timessquare.html (last visited Sept. 21, 2008).

[186] Brief for Plaintiffs-Appellants, *supra* note 181, at 5–6.

[187] *Zieper*, 474 F.3d at 63.

[188] Brief for Defendants-Appellees at 8–9, Zieper v. Metzinger, 474 F.3d 60 (2d Cir. 2007) (No. 05-5250-CV), 2006 WL 4663831. Fitzgerald has since become best known for his efforts as the special prosecutor charged with investigating the leak of covert CIA agent Valerie Plame's name to national media outlets in 2003. *E.g.*, Peter Slevin, *The Prosecutor Never Rests: Whether Probing a Leak or Trying Terrorists, Patrick Fitzgerald Is Relentless*, WASH. POST, Feb. 2, 2005, at C1.

[189] Brief for Defendants-Appellees, *supra* note 188, at 9.

[190] *Zieper*, 474 F.3d at 63.

[191] *Id.* at 63–64.

[192] *Id.* at 64.

[193] *Id.*

First Amendment rights by trying to have the film removed.[194] The attorneys offered to meet with Metzinger, but he declined to discuss the matter further.[195] That was the last contact between federal officials and Zieper or his attorneys.

Prosecutors instead decided to focus their efforts to remove the film on Wieger, who ran the company that hosted Zieper's Web site. They planned to ask Wieger to remove the film pending the completion of their investigation.[196] Then-U.S. Attorney for the Southern District of New York Mary Jo White "emphasized" that the request should be framed as part of the FBI's "good corporate citizenship program, where they, in various contexts, request of citizens to do various things."[197] Metzinger and Lisa Korologos, the Assistant U.S. Attorney assigned to the case, called Wieger on November 15, 1999.[198] They said they were afraid that the film "was going to incite a riot" and that they wanted to move the film offline so that Internet users could no longer access it.[199] They also told Wieger that they had contacted GTE and that if he did not "pull the site down, GTE would."[200] Fearing that he would be arrested and lose his business, Wieger first blocked access to the site and then deleted all of Zieper's files.[201] After several media reports about the affair, Wieger started receiving complaints and threats from people upset by his decision to remove Zieper's film.[202] On November 26, 1999, Wieger made the film available again, and law officials did not contact him about

---

[194] *Id.*

[195] *Id.* at 64.

[196] Brief for Defendants-Appellees, *supra* note 188, at 13.

[197] *Id* at 13.

[198] *Id.* at 14.

[199] *Zieper*, 474 F.3d at 64.

[200] *Id.* (internal quotation marks omitted).

[201] Brief for Plaintiffs-Appellants, *supra* note 181, at 12–14. Wieger's web-hosting company is

> [his] only source of income. Wieger's wife, who has multiple sclerosis, is no longer able to work, and the couple has a legally blind son who needs constant medical attention.
>
> Wieger was afraid that if [the government] went to his upstream providers to take down the film, and told them that he had been uncooperative and was hosting this potentially illegal film, it would have been the immediate end of his business, because his providers could shut his entire business down with the flip of a switch.

Id. at 10 (citations omitted); *see also* Jason Robinson, *Web Site Film Prompts Suit*, SOUTH BEND TRIB., Aug. 10, 2000, at D1 (quoting Wieger as saying he thought the FBI would shut down his company if he did not comply with their requests).

[202] Robinson, *supra* note 201.

taking it back down.[203] Prosecutors subsequently dropped their investigation of Zieper and his film.[204]

Zieper and Wieger brought suit against a handful of federal officials, including Metzinger and Korologos, in December 1999.[205] The district court granted defendants' motion for summary judgment.[206] The court concluded that no reasonable jury could find that Metzinger coerced Zieper in violation of the First Amendment, but that there was a triable issue of fact on the issue of coercion stemming from Metzinger and Korologos's conversations with Wieger.[207] The court then determined, however, that Zieper and Wieger's claims were barred by the doctrine of qualified immunity "because reasonable officers could have disagreed about the legality of" Metzinger and Korologos's actions.[208]

On appeal, the Second Circuit disagreed with the district court that a reasonable jury could not have found that Metzinger's contact with Zieper amounted to a First Amendment violation, but it nevertheless affirmed, holding that Zieper and Wieger's claims were barred by the doctrine of qualified immunity.[209] The Government did not appeal the district court's determination that there was a triable issue of fact regarding possible unconstitutional coercion arising from the defendants' conversations with Wieger—in particular, their statements that the film might incite a riot and that the defendants had already contacted GTE, his upstream provider.[210] On the issue of coercion, then, the appeals court focused solely on Metzinger's contact with the filmmaker Zieper. The court noted that the First Amendment "prohibits government officials from encouraging the suppression of speech in a manner which 'can reasonably be interpreted as intimating that some form of punishment or adverse regulatory action will follow the failure to

---

[203] *Zieper*, 474 F.3d at 65.

[204] Mark Boal, *Subversive Instinct; Times Square Riot Video Back on the Web*, VILLAGE VOICE, Dec. 14, 1999, at 37 (quoting an FBI spokesman as acknowledging that "[n]ot everything that is dangerous or offensive is illegal" and that whether the film was dangerous was no longer "a law enforcement issue").

[205] *Zieper*, 474 F.3d at 65. Zieper and Wieger filed their suit in the U.S. District Court for the District of New Jersey. The court granted the defendants' motion to dismiss Zieper and White's declaratory and injunctive claims on standing grounds, and then transferred the remaining claims—against Metzinger and Korologos in their individual capacities for violating Zieper and White's First and Fifth Amendment rights—to the Southern District of New York. *Id.*

[206] *Id.* (citing Zieper v. Metzinger, 392 F. Supp. 2d 516 (S.D.N.Y. 2005)).

[207] *Id.*

[208] *Id.*

[209] *Id.*

[210] *Id.* at 67 n.3.

accede to the official's request.'"[211] When "determining whether a particular request to suppress speech is constitutional, what matters is the 'distinction between attempts to convince and attempts to coerce.'"[212]

The Second Circuit was also guided by the Supreme Court's decision in *Bantam Books, Inc. v. Sullivan*, in which the Court held that notices sent to book distributors by a Rhode Island state commission prohibiting distribution of indecent and obscene materials to individuals under the age of eighteen amounted to unconstitutional prior restraints on speech.[213] The notices sent by the Rhode Island Commission to Encourage Morality in Youth contained lists of "objectionable" books and magazines, mentioned that the commission had sent the same lists to local police departments, and warned that "[t]he Attorney General will act for us in case of non-compliance."[214] The Court, in holding the notices unconstitutional, noted that they were "phrased virtually as orders" and "provide[d] no safeguards whatever against the suppression of . . . constitutionally protected matter."[215]

Turning to the specifics of Metzinger's interaction with Zieper, the Second Circuit noted that Metzinger never made "clear that Zieper's actions were lawful or that he would not face consequences for making the video public."[216] At the same time, the court acknowledged that Metzinger never expressly threatened Zieper with punishment.[217] But the government's decision, the court continued, "to send not only an FBI agent, but also three police officers, to his home before even speaking with him could have reasonably suggested to someone in Zieper's position that there might be legal consequences if he failed to accede to the government's request that he remove his video."[218] Accordingly, the court held that a rational juror could conclude that the officers' actions were "an attempt to coerce Zieper into removing his film from the internet."[219]

---

[211] *Zieper*, 474 F.3d at 65–66 (quoting Hammerhead Enters., Inc. v. Brezenoff, 707 F.2d 33, 39 (2d Cir. 1983)).

[212] *Id.* at 66 (quoting Okwedy v. Molinari, 333 F.3d 339, 344 (2d Cir. 2003)).

[213] 372 U.S. 58, 71 (1963).

[214] *Id.* at 62 n.5.

[215] *Id.* at 68, 70.

[216] *Zieper*, 474 F.3d at 66.

[217] *Id.*

[218] *Id.* at 67. The court also noted that government officials "repeatedly called" Zieper—twice on the evening they visited his home, and "then again the next day"—and that Metzinger ignored the assertion of Zieper's lawyers that the government's actions violated the First Amendment and refused their offer to meet. *Id.* at 66–67.

[219] *Id.* at 67.

The court then proceeded to the question of whether Metzinger and Korologos were entitled to qualified immunity, explaining that under that doctrine "governmental actors are 'shield[ed] . . . from suits for damages . . . unless their actions violate clearly-established rights of which an objectively reasonable official would have known.'"[220] The court concluded that case law "would not have made apparent to a reasonable officer" that the defendants' conduct was an unconstitutional attempt at coercion "because the cases in which [it has] held that individuals' First Amendment rights were violated involved conduct more likely to be perceived as threatening than that here."[221] The court pointed specifically to *Bantam Books*, explaining that the threats in that case, coming from a state commission and threatening action by the state attorney general in the event of non-compliance, "were much more explicit than those in the present case."[222]

There was nothing inherently threatening, the court reasoned, in Metzinger's statements to Zieper that the film might upset people visiting New York and hurt local businesses, or his asking whether the FBI could prevent people from watching the film.[223] Similarly, the court noted that while Korologos's statement to Wieger about GTE's willingness to take down Zieper's site "could reasonably be interpreted as threatening economic sanctions," Korologos "never indicated that she understood the potential economic significance to Wieger of his relationship with the upstream provider, or suggested that she was using their alleged prior contact to gain leverage."[224] The court also held that a reasonable official could have interpreted the statement that Zieper's film might incite a riot "as simply an explanation of why they were concerned about the video and not a threat of prosecution under the criminal statute."[225] Thus, the court held that Metzinger and Korologos were entitled to qualified immunity because a

---

[220] *Id.* (quoting Thomas v. Roach, 165 F.3d 137, 142 (2d Cir. 1999)).

[221] *Id.* at 68.

[222] *Zieper*, 474 F.3d at 68–69. The court also noted that in *Bantam Books* a separate notice explicitly threatened prosecution: "Your cooperation in removing the listed and other objectionable publications . . . will be appreciated. Cooperative action will eliminate the necessity of our recommending prosecution to the Attorney General's department." *Id.* at 69 (quoting Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 63 n.5 (1963)).

[223] *Id.* at 69.

[224] *Id.* at 70. ("Korologos could have believed that this statement would reasonably be interpreted as only informative. Indeed, at oral argument, appellants' counsel acknowledged that one reasonable inference of Korologos' statement was that she was simply making a factual assertion.").

[225] *Id.*

reasonable officer in their circumstances could have believed that his or her actions were lawful.[226]

The Second Circuit noted that Zieper and Wieger expressed "concern that extending qualified immunity to the officials here will effectively immunize government officials from liability whenever they use ambiguous threats to suppress protected speech, but this fear is unwarranted."[227] The court acknowledged that there would be cases in which "circumstances are such that a reasonable officer would have to recognize that his or her requests could reasonably be interpreted as threatening."[228] And it stressed that its narrow holding only meant that Metzinger and Korologos's "actions here do not present such a case."[229]

With all due respect to the court, its holding in *Zieper* greatly diminishes the First Amendment's protection of online speech. The government's actions in *Zieper* highlight the tremendous power imbalance between federal officials and small-time ISPs such as Wieger's company. In light of that imbalance, innocent-seeming requests—to say nothing of the overt threat in *Zieper* to call an ISP's upstream provider into action—can take on a coercive tone. Consequently, the possibility that such requests will chill online speech is manifest. Additional analysis of the case's ramifications, including suggestions for how better to structure government requests of ISPs, is in Part VI.A.1.[230]

---

[226] *Id.* at 71.

[227] *Id.* at 70.

[228] *Id.*

[229] *Zieper*, 474 F.3d at 70. The court also observed that because of its holding that a juror could reasonably conclude that Metzinger and Korologos's actions violated the First Amendment, "officials who are in a similar situation in the future will be on notice that they must be especially careful to make sure that the totality of their actions do not convey a threat even when their words do not." *Id.* at 70–71.

[230] For an example of government officials pressuring an ISP to remove online content in a different context, see Pilchesky v. Miller, No. 3:CV-05-2074 (M.D. Pa. Aug. 8, 2006). The plaintiffs in *Pilchesky* operated a Web site providing a message board for people to discuss the political scene of Scranton and Lackawanna County, Pennsylvania. *Id.* at 3. After the plaintiffs posted a message critical of the director of Lackawanna County's Office of Economic and Community Development, the director's brother, together with a member of the Pennsylvania State Police and an Assistant District Attorney for Lackawanna County, pressured the plaintiffs' ISP to shut down the message board. *Id.* at 3–4. The ISP complied after getting a letter from the trooper saying he was conducting a criminal investigation of the "harassing posts." *Id.* at 4. The parties eventually settled, with the District Attorney's Office agreeing to pay $50,000 to the American Civil Liberties Union, which represented the plaintiffs in the case. Terrie Morgan-Besecker, *Couple Settle Suit Against Police, DA; Pilcheskys Said Officials Pressured Company To Shut Down Their Political Web Site*, TIMES LEADER, Aug. 15, 2007, at A1.

b. *Statutory Provisions*

In addition to the requests at issue in *Zieper*, which are not statutorily based, recent laws have made it easier for ISPs to voluntarily report questionable material to government authorities. The provisions, included in the Cyber Security Enhancement Act of 2002 ("CSEA"),[231] amended the Electronic Communications Privacy Act of 1986 ("ECPA").[232] They allow a "provider"[233] to divulge the content of communications and subscriber information to any governmental entity "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency."[234] The 2002 amendments significantly reduced the requirements to reveal such information—changing the condition on providers' actions from one of "reasonableness" to one of "good faith," and omitting the condition that the emergency be immediate.[235] The types of subscriber information that an ISP could disclose include: "name, address, billing records, telephone number, records of session times and duration, temporarily assigned network addresses, type of service provided, and means and sources of payment."[236] ISPs that make such disclosures are immune from civil actions based on the ECPA and its amendments.[237]

Additionally, ISPs were already immune from civil liability for any "Good Samaritan" blocking or screening of "objectionable" material under a provision of the Communications Decency Act of 1996 ("CDA").[238] The

---

[231] The CSEA was part of the Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (codified in scattered sections of 18 U.S.C.).

[232] Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

[233] A "provider" is defined as "a person or entity providing an electronic communication service to the public." 18 U.S.C. § 2702(a)(1) (2000).

[234] 18 U.S.C. § 2702(b)(7) (Supp. II 2002).

[235] Birnhack & Elkin-Koren, *supra* note 156, ¶ 104 n.255.

[236] *Id.* ¶ 104.

[237] 18 U.S.C. § 2703(e) (Supp. II 2002) ("No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.").

[238] 47 U.S.C. § 230(c)(2)(A)-(B) (2000). The provision provides that an ISP cannot be held liable for

> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy,

same section also exempts ISPs from civil liability for any harm to third parties caused by information they provide through their services.[239] By giving ISPs carte blanche to regulate content, the complete exemption from liability might appear as a serious threat to unrestricted online speech. But the combination of immunity for self-regulation and immunity for content was Congress's attempt to promote free speech online, while at the same time encouraging ISPs to control the amount of objectionable material they disseminate. Congress feared that, in the absence of immunity from harm caused by their content, ISPs would excessively censor speech to avoid liability.[240] At the same time, Congress wanted to encourage ISPs to self-regulate.[241] Under then-existing case law, ISPs that regulated online content were considered publishers, opening them to liability for content they disseminated.[242] By providing immunity for blocking and screening content, Congress hoped to "remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material . . . ."[243]

Taken together, the self-reporting and self-regulation provisions give ISPs broad authority to divulge to the government questionable content and subscriber information, or simply to censor such content outright. As is discussed in Part VI.A.2, while the First Amendment rationale underlying the

---

excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

Id. The CDA was Title V of the Telecommunications Act of 1996, Pub. L. No. 104-104, §§ 501-61, 110 Stat. 56, 133–43 (codified as amended in scattered sections of 47 U.S.C.). The primary purpose of the CDA was to protect minors from indecent and patently offensive material on the Internet by criminally punishing individuals who transmitted such material to individuals under the age of 18. *Id.* at § 508. The Supreme Court struck down those provisions of the CDA in *Reno v. Am. Civil Liberties Union*, holding that they were unconstitutional content-based regulations that were not narrowly tailored to serve the government's interest. 521 U.S. 844, 868, 882 (1997).

239 47 U.S.C. § 230(c)(1) (2000) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.").

240 Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997) ("The purpose of this statutory immunity is not difficult to discern. Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium.").

241 47 U.S.C. § 230(c)(2) (2000).

242 *Zeran*, 129 F.3d at 330.

243 47 U.S.C. § 230(b)(4) (2000).

self-regulation provisions is sound, the self-reporting provisions could be improved to better address speech and privacy concerns.

2. *Online Speech and Providing "Material Support" to Terrorists*

In its efforts to prevent additional terrorist attacks, the federal government has focused not only on terrorists themselves and their potential plans, but also on individuals who provide "material support" to terrorists.[244] The most commonly used provision prohibits individuals from knowingly providing "material support or resources to a foreign terrorist organization . . . ."[245] "Material support" is defined as "any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel . . . and transportation, except medicine or religious materials."[246]

Plaintiffs successfully attacked the provision in the Ninth Circuit case of *Humanitarian Law Project v. Mukasey* by arguing that some of its terms are unconstitutionally vague.[247] Six organizations, a retired judge, and a surgeon sued the federal government in 1998, arguing, among other things, that the

---

[244] For an insightful and thorough analysis of the development of U.S. material-support laws, see generally Robert M. Chesney, *The Sleeper Scenario: Terrorism-Support Laws and the Demands of Prevention*, 42 HARV. J. ON LEGIS. 1 (2005). Chesney notes that since 9/11 the government has charged nearly 130 individuals with providing material support to terrorists. *See id.* at 20.

[245] 18 U.S.C. § 2339B(a)(1) (Supp. IV 2004). A foreign terrorist organization is any organization designated as such by the Secretary of State. 18 U.S.C. § 2339B(g)(6) (2000). To violate the provision, an individual "must have knowledge that the organization is a designated terrorist organization . . . that the organization has engaged or engages in terrorist activity . . . or that the organization has engaged or engages in terrorism." 18 U.S.C. § 2339B(a)(1) (Supp. IV 2004).

[246] 18 U.S.C. § 2339A(b)(1) (Supp. IV 2004). The federal government's material-support law has gone through several iterations, beginning with the Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, 108 Stat. 1796 (codified as amended at 18 U.S.C. § 2339A (2000)), amended by the Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, 110 Stat. 1214 (codified as amended in scattered sections of 8, 18, 22, 28, and 42 U.S.C.), Patriot Act, *supra* note 2, and then further amended by the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458 §§ 6601–04, 118 Stat. 3638, 3761–64 (codified at 18 U.S.C. § 2339 (Supp. IV 2004)).

[247] 509 F.3d 1122 (9th Cir. 2007) (en banc); *see also* Bob Egelko, *Anti-Terror Law Clipped by U.S. Appeals Court; Parts of Statute Are So Vague They're Unconstitutional*, S.F. CHRON., Dec. 11, 2007, at C3.

material-support provision violated their First Amendment rights.[248] They wanted to provide support only to the "nonviolent and lawful activities" of the Partiya Karkeran Kurdistan ("PKK") and Liberation Tigers of Tamil Eelam ("LTTE"), both of which were designated as foreign terrorist organizations by the U.S. Secretary of State.[249] The plaintiffs alleged that they withheld support for PKK and LTTE out of fear of prosecution under the material-support provision.[250] Specifically, they argued that a court could interpret the terms "training," "expert advice or assistance," "service," and "personnel" in the provision to cover the lawful services that they wanted to provide.[251]

In a decision handed down in late 2007, the Ninth Circuit agreed that the terms "training" and "service," and a portion of the term "expert advice or assistance," were void for vagueness, chilling the plaintiffs' constitutionally protected expression and association.[252] The provision defines "training" as "instruction or teaching designed to impart a specific skill, as opposed to general knowledge."[253] The court found it "highly unlikely that a person of ordinary intelligence" would be able to tell difference between legal and illegal training based on that definition.[254] The court found the term "service," which is not statutorily defined, to be equally problematic. Without a statutory definition as a guide, the court held that an individual could easily determine that the term covers constitutionally protected, i.e., non-terrorism-related, expression and association.[255] As for the term "expert advice or assistance," defined as "advice or assistance derived from scientific, technical or other specialized knowledge,"[256] the court took issue

---

[248] *Humanitarian Law Project*, 509 F.3d at 1126. The case bounced back and forth between the trial and appeals court for nearly a decade, through several revisions of the statute. *Id.* at 1126–27.

[249] *Id.* at 1126 n.1 (noting that the plaintiffs wanted to, among other things, "train members of PKK on how to use humanitarian and international law to peacefully resolve disputes" and "train members of LTTE to present claims for tsunami-related aid to mediators and international bodies").

[250] *Id.*

[251] *Id.* at 1133–36.

[252] *Id.* The court held that the 2004 amendments to the provision cleared up any ambiguity concerning the scope of the term "personnel." *Id.* at 1136.

[253] 18 U.S.C. § 2339A(b)(2) (Supp. IV 2004).

[254] *Humanitarian Law Project*, 509 F.3d at 1134 (noting that "a plaintiff who wishes to instruct members of a designated group on how to petition the United Nations to give aid to their group could plausibly decide that such protected expression falls within the scope of the term 'training'").

[255] *Id.* at 1136.

[256] 18 U.S.C. § 2339A(b)(3) (Supp. IV 2004).

only with the "other specialized knowledge" clause. The court held that while the other parts of the definition are reasonably understandable, expert advice or assistance that includes "other specialized knowledge" covers "constitutionally protected advocacy."[257]

In a separate situation involving Internet content, the vagueness of the material-support provision caused the University of California at San Diego—in its role as ISP to its students—to order a student group to remove links on its Web site, hosted on UCSD computers, to a Web site supporting Fuerzas Armadas Revolucionarias de Colombia ("FARC"), a Colombian group designated by the federal government as a foreign terrorist organization.[258] The school also ordered the group, a "confederation of self-described radical students," to remove content on its site that contained political statements by the PKK, one of the groups at issue in *Humanitarian Law Project*.[259] Administrators were worried that the link and hosted content ran afoul of the material-support provision, particularly given the provision's inclusion of "communications equipment" in its list of banned types of support.[260] After conferring with university lawyers, the school decided to allow the student group to keep the link to FARC, but it still demanded removal of the content supportive of PKK.[261]

The University of California at San Diego's actions illustrate the effect that the material-support provision can have on ISPs. Even when content unequivocally protected by the *Brandenburg* doctrine is involved, the inherent vagueness of the material-support provision can pressure ISPs to err on the side of non-liability and censor the content. Part VI.B. discusses ways to rid the provision of vagueness to protect online speech more fully.

---

[257] *Humanitarian Law Project*, 509 F.3d at 1135.

[258] *University Orders Student Group to Remove Link to a Rebel Group's Web Site*, CHRON. HIGHER EDUC., Oct. 11, 2002, at 33.

[259] Declan McCullagh, *University Backs Down on Link Ban*, CNET NEWS, Oct. 8, 2002, http://www.news.com/University-backs-down-on-link-ban/2100-1023_3-961297.html.

[260] *Id.*

[261] Eleanor Yang, *UCSD Will Allow Students to Keep Disputed Web Links*, SAN DIEGO UNION-TRIB., Oct. 11, 2002, at B2 (quoting a university official as saying that "[l]inks are permissible because they are of such minor consequence that they do not constitute material support"); *see also Students at U. of California at San Diego May Keep Web-Site Links to Terrorist Group, Officials Say*, CHRON. HIGHER EDUC., Oct. 25, 2002, at 35. The university maintained that hosting the PKK content on the university's computer server was a "violation of university policy rather than federal law" and that "[u]niversity resources . . . shouldn't be used to promote terrorist organizations." *Id.*

3. *National Security Letters*

The federal government can also pressure ISPs through the use of National Security Letters ("NSLs"), which require ISPs and other telecommunications firms, under certain circumstances, to comply with FBI requests "for subscriber information and toll billing records information, or electronic communication transactional records in [their] custody or possession . . . ."[262] For the FBI to "request the name, address, length of service, and local and long distance toll billing records of a person or entity," the Director of the FBI, or his designee, must certify that such information is "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by" the First Amendment.[263] The statute does not specify whether such certification is necessary for the FBI to request "electronic communication transactional records."

Despite the ambiguity regarding the certification process for requesting electronic transaction records, the guarantee required for other requests appears to ensure that the FBI can only target consumer information as part of a legitimate investigation. But a report issued in March 2007 by the U.S. Department of Justice's Office of the Inspector General revealed widespread deficiencies in the FBI's handling of NSLs.[264] Following the 2001 terrorist attacks, the report found, the use of NSLs dramatically increased. After issuing roughly 8,500 NSL requests in 2000, the bureau issued 39,000 in 2003, 56,000 in 2004, and 47,000 in 2005.[265] The requests in 2003 to 2005 involved information about 24,937 "U.S. persons," a term that includes holders of work visas, and 27,262 foreigners inside the country.[266]

The report cited three primary reasons for the increase. First, the Patriot Act eliminated the requirement that the information sought by the FBI through an NSL be connected to a "foreign power or agent of a foreign power," substituting the lower standard of being "relevant to an authorized national security investigation."[267] Second, the Patriot Act eliminated the

---

[262] 18 U.S.C. § 2709(a) (2000).

[263] 18 U.S.C. § 2709(b)(1) (2000).

[264] U.S. DEP'T OF JUST., OFFICE OF THE INSPECTOR GEN., A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS (2007). The report was ordered by Congress when it enacted the USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006) (codified as amended in scattered sections of the U.S.C.).

[265] U.S. DEP'T OF JUST., *supra* note 264, at 120.

[266] *Id.* at xxi.

[267] *Id.* at 45.

requirement of NSL approval by high-level officials at FBI headquarters, instead allowing special agents in charge of the FBI's fifty-six field offices to sign off on their use.[268] Third, revised guidelines issued by Attorney General John Ashcroft in 2003 authorized the FBI to issue NSLs during preliminary investigations, expanding their use beyond full investigations.[269]

As NSL use increased, however, the FBI's system of issuing and tracking the requests broke down.[270] The Inspector General's report highlighted a number of serious problems.[271] In a random sample of seventy-seven counterterrorism and counterintelligence investigation files open in four FBI field offices from 2003 to 2005, the Inspector General's staff found nearly as many NSL-related violations of FBI policy and relevant law, twenty-two, as the FBI identified, twenty-six, in reports from *all* FBI headquarters and field offices during the same period.[272] The FBI likely underreported the total number of NSLs issued from 2003 to 2005 by 8,850, or six percent of all requests made during that period, because of poor recordkeeping.[273] There was a basic "unfamiliarity" among FBI agents of the "constraints" built into the Bureau's NSL policy.[274] The FBI regularly

---

[268] *Id.*

[269] *Id.*

[270] R. Jeffrey Smith, *Report Details Missteps in Data Collection*, WASH. POST, Mar. 10, 2007, at A1 (The Inspector General's report did "not accuse the FBI of deliberate lawbreaking. But it depict[ed] the bureau's 56 field offices and headquarters as paying little heed to the rules [for issuing NSLs], and misunderstanding them, as they used the USA Patriot Act . . . to request the telephone records, e-mail addresses, and employment and credit histories of people deemed relevant to terrorism or espionage investigations.").

[271] In the course of its investigation, the Inspector General's staff traveled to FBI field offices in New York, Chicago, Philadelphia, and San Francisco, and interviewed more than fifty FBI employees. In the field offices, the staff studied a sample of seventy-seven counterterrorism and counterintelligence investigation files and 293 NSLs "to determine if the NSLs complied with relevant statutes, Attorney General Guidelines, and internal FBI policy." U.S. DEP'T OF JUST., *supra* note 264, at ix.

[272] *Id.* at xxxiii.

[273] *Id.* at xvii (noting that the Inspector General was "unable to fully determine the extent of the inaccuracies because an unknown amount of data relevant to the period covered by [the] review was lost from the" database of the FBI's Office of the General Counsel "when it malfunctioned").

[274] *Id.* at xxx (describing one situation in which an "FBI analyst was unaware of the statutory, Attorney General Guidelines, and internal FBI policy requirements that NSLs can only be issued during a national security investigation and must be signed by the Special Agent in Charge of the field division").

received unauthorized consumer information.[275] And there was extensive confusion about what types of NSL infractions agents needed to report to the FBI's Office of the General Counsel.[276] Indeed, "the FBI did not issue comprehensive guidance about NSL-related infractions until November 2006," more than five years after Congress enacted the Patriot Act.[277] The report sparked "[b]ipartisan outrage" in Congress and prompted calls to reform the FBI's NSL policy.[278] But recent news stories indicate that similar problems continued at least into 2006.[279]

NSLs have also run into legal trouble. In September 2007, a federal district court in the Southern District of New York declared unconstitutional two NSL-related statutory provisions in a case involving an unidentified ISP that received an NSL demanding production of consumer records.[280] First, the court struck down in its entirety 18 U.S.C. § 2709, the primary provision authorizing the use of NSLs,[281] because the court determined it could not sever an unconstitutional portion of the provision from the rest of the statute.[282] The portion that the court found unconstitutional allows the FBI to prohibit ISPs and other telecommunications companies from disclosing their receipt of an NSL, with the exception of disclosure to counsel, upon the bureau's certification that "otherwise there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any

---

[275] *Id.* at xxxii (noting that in four instances the "FBI received telephone toll billing records information and electronic communication transactional records for longer periods than that specified in the NSL").

[276] U.S. DEP'T OF JUST., *supra* note 264, at xxxiii (noting "frequent exchanges" between FBI attorneys showing "significant confusion about the reporting requirements").

[277] *Id.* at xxxiii–xxxiv.

[278] David Stout, *F.B.I. Head Admits Mistakes in Use of Security Act*, N.Y. TIMES, Mar. 10, 2007, at A1; *see also* Dan Eggen & John Solomon, *FBI Audit Prompts Calls for Reform; Some Lawmakers Suggest Limits on Patriot Act*, WASH. POST, Mar. 10, 2007, at A1.

[279] Dan Eggen, *FBI Chief Confirms Misuse of Subpoenas; Security Letters Used To Get Personal Data*, WASH. POST, Mar. 6, 2008, at A2 (quoting testimony by FBI Director Robert S. Mueller III to the Senate Judiciary Committee that a follow-up report to the 2007 report, to be released sometime in March 2008, will "identify issues similar" to those in the earlier report, but that the time period for the upcoming report "predates the reforms" the FBI has since instituted to prevent further abuse); *see also* Eric Lichtblau, *F.B.I. Says Records Demands Are Curbed*, N.Y. TIMES, Mar. 6, 2008, at A18.

[280] Doe v. Gonzales, 500 F. Supp. 2d 379, 425 (S.D.N.Y. 2007).

[281] *See supra* Part V.B.3.

[282] *Doe*, 500 F. Supp. 2d at 425.

person."[283] The court held that the provision failed to satisfy one of the three procedural safeguards the Supreme Court requires for government-run, content-based licensing schemes.[284]

The Court developed those safeguards in *Freedman v. Maryland*, a case involving a Maryland statute that required movie theaters to submit for approval films they wanted to exhibit, prior to any public showings, to the Maryland State Board of Censors.[285] The board had the power to reject any film it considered "obscene" or that it believed tended to "debase or corrupt morals or incite to crimes."[286] The Court held that such a licensing scheme could survive constitutional scrutiny only if it "takes place under procedural safeguards designed to obviate the dangers of a censorship system."[287] The Court then articulated three required safeguards: (1) the government could restrain a film's exhibition prior to judicial review only "within a specified brief period"; (2) any restraint imposed prior to "final judicial determination" similarly had to be limited to "the shortest fixed period compatible with sound judicial resolution"; and (3) the burden of going to court to challenge a film, and the burden of proof once in court, rested on the government.[288] The Court held that the Maryland statute did not have adequate safeguards because the burden was on the exhibitor to challenge a censor's ruling, showings of films rejected by the board were "prohibited pending judicial review, however protracted," and it provided "no assurance of prompt judicial determination."[289]

Applying *Freedman*, the district court in New York determined that the nondisclosure orders for NSL recipients were content-based licensing schemes, and that they satisfied the first of *Freedman*'s two safeguards because they allowed an NSL recipient to petition a court to modify or set aside such an order.[290] But the court held that it failed the third *Freedman* safeguard because it placed the burden of seeking judicial relief on the NSL recipient.[291] As the court noted, ISPs and other telecommunications companies "generally have little or no incentive to challenge nondisclosure

---

[283] 18 U.S.C. § 2709(c)(1) (2006). The same provision requires NSL recipients to inform the FBI of anyone, with the exception of counsel, that they have told, or plan to tell, about receiving an NSL. 18 U.S.C. § 2709(c)(4) (2006).

[284] *Doe*, 500 F. Supp. 2d at 405–06.

[285] 380 U.S. 51, 52 nn.1–2 (1965).

[286] *Id.* at 52 n.2.

[287] *Id.* at 58.

[288] *Id.* at 58–59.

[289] *Id.* at 59–60.

[290] *Doe*, 500 F. Supp. 2d at 401 (citing 18 U.S.C. § 3511(b) (2006)).

[291] *Id.* at 405–06.

orders" because such challenges are "time consuming and financially burdensome."[292] Indeed, the court noted that "only two challenges have been made in federal court since the original enactment of the statute in 1986."[293] Given the lack of incentive on the part of NSL recipients to challenge such orders, the court concluded that the FBI possessed "broad, unchallenged, and 'in practice . . . final' power" to demand nondisclosure, in violation of *Freedman*.[294]

Applying strict scrutiny, the court also held that the nondisclosure provision lacked the type of narrow tailoring that a content-based restriction needs to avoid constitutional infirmity.[295] In particular, the court noted that the nondisclosure orders "*permanently* restrict an NSL recipient from engaging in *any* discussion related to its receipt of the NSL."[296] The court reasoned that "it is hard to conceive of any circumstances that would justify a permanent bar on disclosure."[297] Once a national security threat posed by disclosure has passed, the court concluded, an NSL recipient should be free to communicate its "knowledge of the government's activities."[298] The court then held that all of § 2709 was unconstitutional because the secrecy of the NSL system intended by Congress could not be achieved without the nondisclosure provision.[299]

---

[292] *Id.* at 405.

[293] *Id.*

[294] *Id.* at 406 (quoting *Freedman*, 380 U.S. at 58). The court noted that although "the government bears the burden of justifying the need for nondisclosure to a court," that "does not mean that the FBI must obtain the approval of a court prior to issuing an NSL with a nondisclosure order." *Id.* Rather, "the FBI may issue a temporary nondisclosure order on its own . . . provided that, within a reasonable and brief period of time, it must either notify the NSL recipient that the order is no longer in effect, or justify to a court the need for a continued period of nondisclosure." *Id.*

[295] *Id.* at 425.

[296] *Doe*, 500 F. Supp. 2d at 420. To illustrate the sweeping nature of a nondisclosure order, the court noted

> [that] an NSL recipient cannot communicate to anyone indefinitely that it received an NSL, the identity of the target, the type of information that was requested and/or provided, general statistical information such as the number of NSLs it received in the previous month or year, its opinion as to whether a particular NSL was properly issued in accordance with the applicable criteria, or perhaps even its opinion about the use of NSLs generally.

Id.

[297] *Id.* at 421.

[298] *Id.*

[299] *Id.* at 424.

Additionally, the court found unconstitutional 18 U.S.C. § 3511(b), the provision providing judicial review of NSL nondisclosure orders, because it violated the doctrine of separation of powers and the First Amendment.[300] The provision provides that a court may modify or set aside such an order only if it "finds that there is no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person."[301] The court held that the provision improperly interfered with its ability to fully scrutinize nondisclosure orders and is "plainly at odds with First Amendment jurisprudence which requires that courts strictly construe content-based restrictions and prior restraints to ensure they are narrowly tailored to advance a compelling government interest."[302]

Given the numerous abuses detailed in the Inspector General's report and the legal infirmities highlighted by the district court in New York, the FBI's entire NSL program is suspect. Aside from the privacy concerns of individuals whose personal information is sought through NSL requests, a topic that is outside the scope of this Note, the NSL system also directly threatens the First Amendment rights of ISPs, and increases the likelihood of censorship of constitutionally protected material by ISPs intimidated by government requests for subscriber information. Part VI.C of this Note discusses potential solutions to the NSL threat.

VI. A WAY FORWARD: PROTECTING ISPS FROM GOVERNMENT COERCION

A number of federal laws and policies, highlighted above, "threaten to recruit" ISPs as "a federally conscripted corps of censors."[303] The government's intense interest in terrorism-related Internet content, coupled with its pressure on ISPs, endangers speech that is clearly protected by the *Brandenburg* doctrine, as illustrated in the *Zieper* case[304] and the University of California at San Diego's efforts to scrub core political speech from its servers.[305] The goal of this Note, however, is not to argue that there should be no cooperation between the government and ISPs in the effort to police the Internet for illegal content. Rather, its purpose is to urge that cooperation

---

[300] *Id.* at 425.

[301] 18 U.S.C. § 3511(b)(2) (2006).

[302] *Doe*, 500 F. Supp. 2d at 409.

[303] Kreimer, *supra* note 24, at 93.

[304] *See supra* Part V.B.1.a.

[305] *See supra* Part V.B.2.

between the public and private sectors in this area should not come at the expense of constitutionally protected speech.[306] This Part recommends ways to achieve a healthier balance between the government and ISPs.

A. *Recommendations for "Good Corporate Citizen" Programs and Provisions*

1. *Government Requests To Remove Online Content*

Government officials who request ISPs to remove online content, such as the officials in *Zieper*, should have to affirmatively state that they lack the legal authority to compel removal of the content and, furthermore, that ISPs are immune from prosecution if they choose to decline the request.[307] By the time officials contacted Mark Wieger, the owner of the small ISP that hosted Michael Zieper's film, they knew that the film was constitutionally protected and that they could not order its removal.[308] Yet, because of the tremendous power imbalance between the government officials and Wieger, those requests came off as threats.[309] Wieger feared prosecution and the loss of his business.[310] In fact, many ISPs are small-time players like Wieger, "weak links in the chain of communications" who simply find it easier to drop a

---

[306] Professor Zittrain, who generally sees substantial promise in the growing cooperation between the government and ISPs, has argued, for example, that greater government control of Internet intermediaries "cannot be accepted, even if initiated for substantively good intentions, without the most exacting of processes to avoid abuse, including a comprehensive framework where sovereigns' actions to block material are thoroughly documented and open to challenge." Zittrain, *supra* note 147, at 688.

[307] *See* Brief for Volunteer Lawyers for the Arts as Amicus Curiae Supporting Plaintiffs-Appellants at 26, Zieper v. Metzinger, 474 F.3d 60 (2d Cir. 2007) (No. 05-5250-CV). Arguing for such a requirement, Volunteer Lawyers for the Arts maintained that the

> First Amendment's right to free expression certainly is a fundamental Constitutional right that warrants safeguards, and if law enforcement is permitted to continue its unchecked requisitions of self-censorship, the burden on law enforcement officers to affirmatively inform the citizenry not only that they lack any authority to compel, but that the citizen is immune from any government retaliation if she chooses to ignore the "recommendation" would be slight. The offsetting benefit of the breathing room to expression it would create substantially outweighs the burden on government.

Id.

[308] *Zieper*, 474 F.3d at 63.

[309] *See supra* note 192 and accompanying text.

[310] *Id.*

troublesome customer or censor speech than risk government penalties.[311] Requiring government officials to reveal their lack of authority to compel removal of online material or to retaliate for an ISPs decision to decline a request would not unduly burden the officials, and would put the ISP on better footing to make a reasoned evaluation of the request. Given the value of constitutionally protected speech, such a change in policy is not too much to ask.

2. *Statutory Provisions*

The rationale behind the provisions of the Communications Decency Act of 1996 that provide immunity to ISPs for the content they carry and encourage self-regulation of content—namely, that exposing ISPs to liability would chill speech on the Internet—is sound, and Congress should not alter those provisions.[312]

Congress does need to amend, however, the provision in the Cyber Security Enhancement Act of 2002 that makes it easier for an ISP to voluntarily divulge consumer information to governmental authorities.[313] As it currently stands, the provision allows an ISP to divulge the content of communications and subscriber information to any governmental entity "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency."[314] Congress should return the provision to its pre-2002 form, which contained a "reasonableness" standard, rather than a "good faith" standard, and required that the emergency be "immediate."[315] Particularly because of the pressure that the federal government is applying to ISPs in other areas of the law—through the material-support-for-terrorism provision[316] and the use of National Security Letters,[317] for example—the current provision increases the likelihood that ISPs will target constitutionally protected speech and invade user privacy to avoid any possibility of government sanction.

---

311 Kreimer, *supra* note 24, at 28–29, 70.

312 *See supra* Part V.B.1.b and text accompanying notes 238, 239 & 241.

313 *See supra* Part V.B.1.b.

314 18 U.S.C. § 2702(b)(8) (2006).

315 *See supra* Part V.B.1.b.

316 *See supra* Part V.B.2.

317 *See supra* Part V.B.3.

B. *Recommendation for the "Material-Support" Provision*

A cloud of confusion surrounds the most used provision prohibiting "material support" of terrorism, 18 U.S.C. § 2339B. The Ninth Circuit recently held that a number of terms in the provision's definition of "material support"—specifically, "training," "service," and "expert advice or assistance"—are unconstitutionally vague.[318] The University of California at San Diego ordered a student group to remove a link on its Web site to a designated foreign terrorist organization because it feared that the link could fall under the term "communications equipment" in the material-support definition.[319] While it is true that the government tried and failed to convict an Idaho graduate student for publishing speeches and other materials supporting terrorism on the Internet,[320] without further guidance from Congress on the meaning of "material support," doubts will remain about what types of expression, if any, are barred by the provision.

One solution could be for Congress to more precisely define the terms already in the provision by fleshing out, for example, what it means by "training" and "service." But trying for such precision could be difficult and self-defeating. An easier and more effective solution would be to expressly state in the provision that speech protected by the First Amendment is excluded from § 2339B's terms.[321] While such an amendment would not clear up all of § 2339B's ambiguities, it would at least be a large step in the right direction. Granted, the University of California at San Diego eventually backed off of its demand for the student group to remove the link, suggesting that other ISPs can also correctly interpret the provision's terms. But that was only after consulting with the university's lawyers.[322] It is not a stretch to conjecture that many ISPs —such as Mark Wieger in the *Zieper* case [323]—do

---

[318] *See supra* Part V.B.2.

[319] *See supra* Part V.B.2.

[320] *See supra* Part V.A.

[321] *See* Chesney, *supra* note 244, at 83 (making the same recommendation and stating that "[s]uch activity may provide a predicate for an investigation, but by definition it would be unconstitutional to prosecute on this basis, and there can be no harm in saying so in the statutes themselves"). Daniel Bryant, the Assistant Attorney General for Legal Policy, offered a similar recommendation in testimony before the Senate Judiciary Committee. *Aiding Terrorists:An Examination of the Material Support Statute Before S. Judiciary Comm.*, 108th Cong. (2004) (statement of Daniel Bryant, Assistant Attorney General, U.S. Department of Justice). Bryant said that "such a provision would have no effect on current prosecution policy, which does not target conduct protected by the First Amendment." *Id.* at 122.

[322] *See supra* Part V.B.2.

[323] *See supra* Part V.B.1.a.

not have teams of lawyers ready at their disposal and are more likely to opt for the path of least resistance and remove questionable content. A clause in the material-support provision explicitly exempting constitutionally protected speech could help prevent such censorship.

C. *Recommendations for the FBI's Use of National Security Letters*

As the report of the Department of Justice's Inspector General[324] and the recent decision of the district court in the Southern District of New York[325] make clear, the FBI's system of issuing and using National Security Letters is broken. From 2003 to 2005, the FBI underreported the total number of NSLs it issued.[326] It obtained consumer information from improper investigations.[327] It obtained unauthorized consumer information.[328] And it did not properly instruct FBI employees about what types of activities constituted violations of the bureau's NSL policy.[329] Its system suffers from constitutional problems, as well. The district court held that the primary statute authorizing the use of NSLs violated the First Amendment because it permanently bars NSL recipients from disclosing the fact that they received an NSL,[330] and because it places the burden on NSL recipients to challenge nondisclosure orders in court.[331] Additionally, the court held that another NSL provision was unconstitutional because it mandates a lower standard of review of nondisclosure orders for courts than the First Amendment requires.[332]

The FBI's NSL program allows the government to monitor Internet users and bars ISPs from letting them know, not just at the time of any investigation, but permanently, imperiling the users' and ISPs' First Amendment rights alike, and chilling conversation about an investigatory tool that has been subject to rampant abuse.[333] What is more, the receipt of

---

[324] *See supra* Part V.B.3.

[325] *See id.*

[326] *See supra* Part V.B.3 and note 270.

[327] *See supra* Part V.B.3 and note 271.

[328] *See supra* Part V.B.3 and note 272.

[329] *See supra* Part V.B.3 and note 273.

[330] *See supra* Part V.B.3.

[331] *See id.*

[332] *See id.*

[333] *See* Doe v. Gonzales, 500 F. Supp. 2d 379, 395 (S.D.N.Y. 2007). In striking down 18 U.S.C. § 2709, the judge wrote:

> In light of the seriousness of the potential intrusion into the individual's personal affairs and the significant possibility of a chilling effect on speech and association—

an NSL essentially puts an ISP on notice that one of its subscribers is the subject of a federal investigation, increasing the probability that the ISP will drop the subscriber to avoid liability. But as the Inspector General's report illustrates, the fact that the FBI issues an NSL does not mean that the investigation is legitimate.

Fixing the NSL program would require, as a start, addressing two of the primary drivers behind the rapid increase in the use of NSLs. First, Congress should return to the pre-Patriot Act framework of only allowing high-level officials at FBI headquarters to approve the issuance of NSLs, rather than the current framework that allows agents in charge of field offices to approve NSLs. Many of the issues highlighted in the Inspector General's report were the result of general confusion about NSL policy among staff in FBI field offices,[334] a problem that could be alleviated if FBI officials more familiar with the policy had a tighter control of the program. Second, the Justice Department should return to the pre-2003 framework when NSLs could be used only in full investigations, and not in preliminary investigations, as is currently allowed.[335] Gathering subscriber information without their knowledge should be used only when there is a solid basis for an investigation, and not as a kind of fishing expedition, which is the general picture that emerged from the Inspector General's report. By rolling back these changes that led to the surge in NSL use, the FBI can regain control of the program and better protect the rights of ISPs and subscribers.[336]

Additionally, Congress should amend the NSL provisions in accordance with the district court's ruling in the Southern District of New York. First, it should amend 18 U.S.C. § 2709(c) to allow an ISP to disclose that it received

---

particularly of expression that is critical of the government or its policies—a compelling need exists to ensure that the use of NSLs is subject to the safeguards of public accountability, checks and balances, and separation of powers that our Constitution prescribes.

Id.

[334] *See supra* p. 42 and note 271.

[335] *See supra* Part V.B.3.

[336] The author of this Note does not think it is necessary to roll back the third major cause of increased NSL usage: the change in the requirement that NSLs had to relate to a "foreign power or agent of a foreign power" to the requirement that they had to be "relevant to an authorized national security investigation." *See* U.S. DEP'T OF JUST., *supra* note 262, at 45. Given the rise in decentralized terrorist networks not affiliated with specific countries, the government has a clear interest in investigating potential terrorist activity by individuals affiliated with such networks. Furthermore, by putting the power to approve NSLs back into the hands of high-level FBI officials, and by allowing their use only in full investigations, it is this author's position that many of the program's problems could be fixed.

an NSL once any national security threat has passed.[337] As the court noted, "[o]nce disclosure no longer poses a threat to national security, there is no basis for further restricting NSL recipients from communicating their knowledge of the government's activities."[338] Second, Congress should put the burden on the government, rather than ISPs, to justify the need for nondisclosure in the courts. This is particularly important in light of the court's observation—supported by evidence in the Inspector General's report—of the extreme disincentive on the part of ISPs to challenge nondisclosure orders.[339] Third, Congress should repeal the provision that limits courts' scrutiny of nondisclosure orders.[340] The orders are content-based restrictions and prior restraints on speech, and courts should review them using strict scrutiny.

VII. CONCLUSION

One of the most pernicious aspects of the type of pressure that the government places on ISPs is that the vast majority of it takes place out of public view. Few ISPs challenge the government in litigation[341] or otherwise gain notoriety for their attempts at censorship. But those situations that do become public—such as Mark Wieger pulling Michael Zieper's film offline,[342] or the University of California at San Diego confronting a student group over links on its Web site[343]—offer disturbing glimpses of ISPs' reactions to government policies. The tendency is for ISPs "to engage in broadly prophylactic responses" to regulations,[344] to make the easy choice of dropping a troublesome subscriber or turning over customer information to the FBI. And because it takes place in private, whether by choice or by government fiat, the debate that should be occurring about these developments is not.

Growing government influence over ISPs is particularly troubling when it comes to terrorism-related online speech that should fall under the protection of the *Brandenburg* doctrine. What the government cannot get directly—punishment in court for a speaker who advocates terrorism but does not come close to violating *Brandenburg*—it can pursue by coercing the

---

[337] *See supra* Part V.B.3.

[338] *Doe*, 500 F. Supp. 2d at 421.

[339] *See supra* pp. 44–45.

[340] *See supra* Part VI.

[341] Kreimer, *supra* note 24, at 65.

[342] *See supra* Part V.B.1.a.

[343] *See supra* Part V.B.3.

[344] Kreimer, *supra* note 24, at 65.

companies that host the speeches and appeals or transmit the private conversations of the speaker. To allow proxy censorship, as opposed to direct censorship, does no less damage to *Brandenburg*, a doctrine built up by the Supreme Court through two World Wars and the Red Scare.[345] To turn our backs on the lessons embedded in that test because of the fears of this era, of terrorism and of its relationship with the Internet, would be a disservice to the long history of expanding free-speech rights in this country. That is especially true in light of the Court's statement more than ten years ago that the Internet is home to "vast democratic forums" and deserving of the highest level of First Amendment protection.[346]

Justice Douglas, writing in dissent in *Dennis v. United States* in 1951, recognized the damage that fear can do to the First Amendment. Douglas argued that the defendants in that case, members of the Communist Party of the United States, were being punished not for speech related to any specific or even likely threat against this country, but "because Soviet Russia and her Red Army are a threat to world peace."[347] For Douglas, that was not enough. He reasoned that punishment for speech "must be based on more than fear, on more than passionate opposition against the speech, on more than a revolted dislike for its contents."[348]

Fear led to numerous policy and legal misjudgments by the federal government in the wake of 9/11. In the context of this Note, that fear is infused in the vagueness of the material-support provision, and in the sweeping powers of the FBI's NSL program. At this stage after 9/11, it is time to fix those misjudgments. Fear, as the tortuous path leading to *Brandenburg* illustrates, has not served First Amendment jurisprudence well in the past, and it should not guide us now.

---

[345] *See supra* Part II.

[346] Reno v. Am. Civil Liberties Union, 521 U.S. 844, 868, 870 (1997).

[347] 341 U.S. 494, 588 (1951) (Douglas, J., dissenting).

[348] *Id.* at 585.